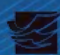


高等学校数学系列教材

近世代数基础

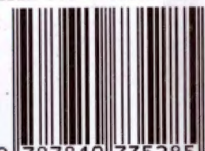
主编/范崇金



哈尔滨工程大学出版社
Harbin Engineering University Press

责任编辑 程小东
封面设计 张　骏

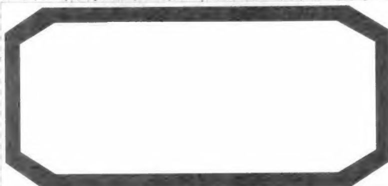




ISBN 978-7-81073-528-5

9 787810 735285 >

定价：15.00元





高等学校数学系列教材

近世代数基础

主编/范崇金



哈尔滨工程大学出版社
Harbin Engineering University Press

内 容 简 介

本书作为工科院校研究生用的近世代数教材，介绍了代数运算、群、环、域及格与布尔代数的基础知识，内容简明扼要。

本书也可作为应用数学专业短学时的近世代数教材和参考书。

图书在版编目(CIP)数据

近世代数基础/范崇金主编.—哈尔滨:哈尔滨工程大学出版社,2003

ISBN 978-7-81073-528-4

Ⅰ.近… Ⅱ.范 Ⅲ.抽象代数-研究生-教材

Ⅳ.O153

中国版本图书馆 CIP 数据核字(2003)第 002536 号

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 哈尔滨工业大学印刷厂
开　　本 787mm×960mm 1/16
印　　张 7.25
字　　数 130 千字
版　　次 2008 年 7 月第 2 版
印　　次 2008 年 7 月第 2 次印刷
定　　价 15.00 元
http://press.hrbeu.edu.cn
E-mail:heupress@hrbeu.edu.cn

前言

在我校研究生教材建设专项资金的资助下，本书得以出版。

随着计算机科学和信息科学的飞速发展，许多学科和领域要处理离散的数学结构——代数结构，有些学科甚至需要较深的近世代数知识。许多工科专业，特别是计算机科学专业的研究生急需开设近世代数课程。近世代数原为数学系一门较难的专业课。目前，绝大多数近世代数教材都是针对数学专业的。数学专业的教材以培养学生的数学素养、以数学研究为最终目的，追求纯数学的完美，篇幅浩大。显而易见，这样的教材是不适合工科研究生的。鉴于此，本书作者，在工科研究生教学和应用数学本科专业教学的基础上编写了此书。

编写教材，写厚容易，写薄难，对于一门36学时的课程更是如此。更难的是，如何使一门极其抽象的数学课程适合工科学生。鉴于本书的对象及学时所限，作者参阅了许多国内外优秀教材，以基础知识为本，尽力以最合理的安排和最新的处理使本教材简明扼要、通俗易懂、突出核心内容和骨干结构。近世代数的核心内容极其抽象，为使学生不致感到太枯燥，为增加学习兴趣，也为了展示近世代数应用的潜力，我们选择介绍了近世代数在几个方面的简单应用。

我校戴遗山教授和唐向浦教授审阅了本书的初稿，提出了非常好的建议，在此向他们表示由衷的感谢。限于作者的能力及知识视野，书中的不当之处在所难免，欢迎各方面的批评和建议。

全书授课时数需要约48学时；没标有☆号的内容可以构成一个36学时的简明教程。由于近世代数的习题较难，本书在最后对习题，特别是证明题给出了较详细的解答。标有*号的习题较难，只供有兴趣的学生练习。

哈尔滨工程大学理学院

编　者

目录



第1章　基本概念

在中学代数中,我们的运算对象是实数或复数.在大学的线性代数中,我们又将运算对象扩大到了向量和矩阵,而且我们已经注意到,这是很有意义的.随着许多新的科学领域的出现,及其数学本身的需要,我们必须将运算的对象进一步扩大.事实上,在现代代数学中,什么东西都可成为我们的运算对象.在本课程中,我们主要学习近世代数学中三个最主要的对象——群、环、域,它们都是在一个集合上定义一些运算律后而成的代数结构.为此,本章中我们介绍集合和运算的基本概念,为后几章中群、环、域的学习打基础.

1.1　集合与映射

1　集合

集合:一般我们将具有某种特性的事物的全体称为一个**集合**.通常我们用大写英文字母 A,B,C 等表示集合.集合中的事物称为元素.我们用 $a\in A$ 表示 a 是集合 A 中的**元素**,读"a 属于 A";$a\notin A$ 表示 a 不是集合 A 中的元素,读"a 不属于 A".

例如,$1\in\{0,1\}$,$2\notin\{0,1\}$.

我们用 $\mathbf{N},\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$ 分别表示自然数集合,整数集合,有理数集合,实数集合和复数集合.这些集合中去掉0后用 $\mathbf{N}^*,\mathbf{Z}^*,\mathbf{Q}^*,\mathbf{R}^*,\mathbf{C}^*$ 表示.

空集:我们称没有元素的集合为**空集**.空集的符号为 $\varnothing$.

例如,$\{x\in\mathbf{R}\mid x^2+1=0\}=\varnothing$

子集:若集合 B 中的元素都属于集合 A,我们称 B 是 A 的**子集**,记为 $B\subset A$.若 B 是 A 的子集,但 $B\neq A$,我们称 B 是 A 的真子集.

例如,若 $A=\{0,1,2\}$,$B=\{0,1\}$,则 $B\subset A$.

注意:对任何集合 A,有

$$\varnothing\subset A,A\subset A.$$

集合的并:对于集合 A,B,我们称集合

$$A\cup B=\{c\mid c\in A\text{ 或 }c\in B\}$$

为 A,B 的**并集**.

例如,$\{0,1,2\}\cup\{1,2,3\}=\{0,1,2,3\}$.

注意:对于集合 A,B,有

$$A \subset A \cup B, B \subset A \cup B.$$

集合的差:对于集合 A,B,我们称集合

$$A - B \equiv \{c \mid c \in A \text{ 且 } c \notin B\}$$

为 A 与 B 的**差集**.

例如,$\{0,1,2\} - \{1,2,3\} = \{0\}$.

集合的交:对于集合 A,B,我们称集合

$$A \cap B \equiv \{c \mid c \in A \text{ 且 } c \in B\}$$

为 A,B 的**交集**.

例如,$\{0,1,2\} \cap \{1,2,3\} = \{1,2\}$.

注意:对于集合 A,B,有

$$A \cap B \subset A, A \cap B \subset B.$$

集合的积:对于集合 A,B,我们称集合

$$A \times B \equiv \{(a,b) \mid a \in A, b \in B\}$$

为 A,B 的**积**.

例如,

$$\{0,1,2\} \times \{a,b\} = \{(0,a),(0,b),(1,a),(1,b),(2,a),(2,b)\};$$

$\mathbf{R}^2 \equiv \mathbf{R} \times \mathbf{R}$ 为平面点集.

2　映射

约定:以后,若无特别声明,集合都不是空集.

定义　对两个集合 A,B.若一个法则 σ 使得 A 中任何一个元素 a 都对应 B 中唯一的一个元素 b,则我们称 σ 为集合 A 到集合 B 的一个**映射**;元素 b 称元素 a 在映射 σ 下的**像**,记为 $\sigma(a) = b$;元素 a 称元素 b 在映射 σ 之下的一个**原像**;若 $A' \subset A$,集合

$$\sigma(A') \equiv \{\sigma(a) \mid a \in A'\} \subset B$$

称 A' 在 σ 下的**像集**;若 $B' \subset B$,集合

$$\sigma^{-1}(B') \equiv \{a \in A \mid \sigma(a) \in B'\} \subset A$$

称 B' 在映射 σ 下的**原像集**.

例 1　设 $A = \{0,1,2,3\}, B = \{a,b,c\}$.

若令

$$\alpha: 0 \mapsto a, 1 \mapsto b, 2 \mapsto a, 3 \mapsto b, 0 \mapsto c$$

则 α 不是 A 到 B 的映射,因为 $0 \in A$ 对应的元素不唯一.

若令

$$\beta: 0 \mapsto a, 1 \mapsto b, 2 \mapsto c$$



则 β 不是 A 到 B 的映射，因为 $3 \in A$ 不对应 B 中的任何元素．

若令

$$\gamma: 0 \longmapsto a, 1 \longmapsto b, 2 \longmapsto a, 3 \longmapsto b,$$

则 γ 是 A 到 B 的映射；此时

$$\gamma(A) = \{a, b\}, \gamma(\{0,2\}) = \{a\}, \gamma(\{0\}) = \{a\},$$
$$\gamma^{-1}(\{a\}) = \{0,2\}, \gamma^{-1}(\{c\}) = \varnothing$$

例 2 $\sigma:(m,n) \longmapsto m+n$ 为 $\mathbf{Z} \times \mathbf{Z}$ 到 $\mathbf{Z}$ 的一个映射．

例 3 令 $M_{m\times n}(\mathbf{R})$ 为一切 $m \times n$ 实矩阵构成的集合，则

$$\sigma:(A,B) \longmapsto AB$$

为 $M_{l\times m}(\mathbf{R}) \times M_{m\times n}(\mathbf{R})$ 到 $M_{l\times n}(\mathbf{R})$ 的一个映射．

定义 设 σ 为集合 A 到集合 B 的一个映射．

(1) 若 $\sigma(A) = B$，即 B 中每个元素在映射 σ 下都至少有一个原像，则我们称 σ 为**满射**；

(2) 若 A 中任何两个不同的元素 a_1, a_2 的像 $\sigma(a_1), \sigma(a_2)$ 也不同，则我们称 σ 为**单射**；

(3) 若 σ 既是单射又是满射，则称 σ 为**双射**．此时我们称 A 与 B **一一对应**；

(4) 集合 A 到自身的映射称 A 的一个**变换**．同理，变换有**单变换**、**满变换**和**一一变换**之分．

例 4 设 $S = \{0,1,2\}, B = \{a,b\}, C = \{a,b,c\}, D = \{a,b,c,d\}$．令

$$\beta: S \to B, 0 \longmapsto a, 1 \longmapsto b, 2 \longmapsto a;$$
$$\gamma: S \to C, 0 \longmapsto a, 1 \longmapsto b, 2 \longmapsto c;$$
$$\delta: S \to D, 0 \longmapsto a, 1 \longmapsto b, 2 \longmapsto c.$$

则 β 是满射，不是单射；γ 是双射，δ 是单射，不是满射．

例 5 设 $A = \{0,1,2,\cdots\}, B = \{0,2,4,\cdots\}$，则 $\sigma: n \longmapsto 2n$ 为 A 到 B 的一个双射，即 A 与 B 一一对应．

例 6 设 $A = [0,2\pi), B = \{(x,y) \in \mathbf{R} \times \mathbf{R} \mid x^2 + y^2 = 1\}$，则

$$\sigma: \theta \longmapsto (\cos\theta, \sin\theta)$$

为 A 到 B 的一个双射．

例 7 集合 A 的一一变换 $1_A: a \longmapsto a$ 称 A 的**恒同变换**．

3 映射的复合

定义 给定两个映射 $\alpha: A \to B$ 和 $\beta: B \to C$，则对应

$$\beta\alpha: A \to C, a \longmapsto \beta(\alpha(a))$$

为 A 到 C 的映射，称其为 α 与 β 的**复合(映射)**．

例 8 设 $A = \mathbf{R}, B = \mathbf{R}^+$ (正实数的集合)．令

$$\alpha: A \to B, x \longmapsto \mathrm{e}^x; \beta: B \to A, y \longmapsto \ln y,$$

则

$$\beta\alpha: A \to A, x \mapsto e^x \mapsto \ln(e^x) = x,$$
$$\alpha\beta: B \to B, y \mapsto \ln y \mapsto e^{\ln y} = y,$$

即 $\beta\alpha = 1_A, \alpha\beta = 1_B$.

定理 映射 $\alpha: A \to B$ 是双射 $\Leftrightarrow$ 存在映射 $\beta: B \to A$ 使

$$\alpha\beta = 1_B, \quad \beta\alpha = 1_A.$$

证明 ($\Rightarrow$) 由于 α 是满射,又是单射,因而对任意 $b \in B$,在 A 中存在唯一一个元素 a 使 $\alpha(a) = b$.令 $\beta: b \mapsto a$,即

$$\beta(b) = a \Leftrightarrow \alpha(a) = b,$$

此时,直接验证可得到 $\alpha\beta = 1_B, \beta\alpha = 1_A$.

($\Leftarrow$) 对任意 $b \in B$,我们有 $(\alpha\beta)(b) = 1_B(b) \Rightarrow \alpha(\beta(b)) = b$,这说明 α 是满射;又

$$\alpha(a_1) = \alpha(a_2) \Rightarrow \beta(\alpha(a_1)) = \beta(\alpha(a_2)) \Rightarrow (\beta\alpha)(a_1) = (\beta\alpha)(a_2)$$
$$\Rightarrow 1_A(a_1) = 1_A(a_2) \Rightarrow a_1 = a_2,$$

这说明 α 是单射.总之,α 是双射.

习题 1－1

1. 若 $A \subset B$,求 $A \cap B, A \cup B$.
2. 试证有理数集合 $\mathbf{Q}$ 与整数集合 $\mathbf{Z}$ 一一对应.
3. 试建立一个由区间 $(0,1)$ 到区间 $(-\infty, +\infty)$ 的一一对应.
4. 证明集合运算律:$U-(A \cup B) = (U-A) \cap (U-B)\ (A, B \subset U)$.
5. 若集合 A 有 n 个不同的元素,证明 A 有 2^n 个不同的子集.

1.2 代数结构

1 代数运算

我们知道对于二维向量有两个运算,一个是数乘向量:

$$k \circ (a, b) = (ka, kb);$$

另一个是向量与向量的加法:

$$(a, b) \oplus (c, d) = (a+c, b+d).$$

事实上,我们可将数乘向量视为一个由 $\mathbf{R} \times \mathbf{R}^2$ 到 $\mathbf{R}^2$ 的映射:

$$\circ: (k, (a, b)) \mapsto (ka, kb),$$

只要将 $\circ(k, (a, b))$ 记为 $k \circ (a, b)$;同样,可将向量与向量的加法视为一个由 $\mathbf{R}^2 \times \mathbf{R}^2$ 到 $\mathbf{R}^2$ 的映射:

$$\oplus: ((a, b), (c, d)) \mapsto (a+c, b+d),$$

只要将 $\oplus((a,b),(c,d))$ 记为 $(a,b)\oplus(c,d)$.

定义 (1) 我们称映射 $\circ: A\times B\to D$ 为 $A\times B$ 到 D 的一个**代数运算**.为了方便,我们用 $a\circ b$ 表示 $\circ(a,b)$;

(2) 由 $A\times A$ 到 A 的一个代数运算 $\circ$ 称为 A 上的一个**二元运算**,此时我们说 $(A,\circ)$ 是一个**代数结构**.

例 1 令 $\circ:(m,n)\mapsto \frac{m}{n}$,则 $\circ$ 为由 $\mathbf{Z}\times\mathbf{Z}^*$ 到 $\mathbf{Q}$ 的一个代数运算,也就是普通的整数除法.

例 2 $\oplus:(m,n)\mapsto m+n$ 为 $\mathbf{Z}$ 上的一个二元运算,也就是普通的整数加法.

例 3 若 $p(A)=\{B\mid B\subset A\}$,则集合的并($\cup$)和交($\cap$)为 $p(A)$ 上的两个二元运算.

2 运算表

当 $A=\{a_1,\cdots,a_n\}$, $B=\{b_1,\cdots,b_m\}$ 为有限集时,若 $\circ$ 为 $A\times B$ 到 D 的代数运算,$a_i\circ b_j=d_{ij}\in D$,我们可用下表表示这个代数运算:

$\circ$	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
a_2	d_{21}	d_{22}	$\cdots$	d_{2m}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

例 4 $A=\{N,Y\}$.在 A 上如下定义两个二元运算 $\otimes$ 和 $\oplus$:

$$Y\otimes Y=Y, Y\otimes N=N, N\otimes Y=N, N\otimes N=N;$$
$$Y\oplus Y=Y, Y\oplus N=N, N\oplus Y=N, N\oplus N=N;$$

它们用运算表表示如下:

$\otimes$	N	Y
N	N	N
Y	N	Y

$\oplus$	N	Y
N	N	Y
Y	Y	Y

例 5 令 $\varepsilon_1=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}$, $\varepsilon_2=\varepsilon_1^2$, $U_3=\{1,\varepsilon_1,\varepsilon_2\}$,则 U_3 对于复数的乘法构成一个代数结构,其运算表如下:

·	1	ε_1	ε_2
1	1	ε_1	ε_2
ε_1	ε_1	ε_2	1
ε_2	ε_2	1	ε_1

习题 1－2

1. 设 $A=\{a,b,c\}$，规定 A 的两个不同的二元运算.

2. $U_6\equiv\{z\in\mathbf{C}\mid z^6=1\}$，写出代数结构$(U_6,\cdot)$的乘法表，这里运算是复数的乘法.

3. $A=\{a,b\}$，写出代数结构$(p(A),\cup)$和$(p(A),\cap)$的运算表.

4. $A=\{0,1,2\}$. 对任意 $a,b\in A$，定义 $a\oplus b$ 为 $a+b$ 被 3 除得到的余数；定义 $a\otimes b$ 为 $a\cdot b$ 被 3 除得到的余数. 写出代数结构$(A,\oplus)$和$(A,\otimes)$的运算表.

1.3 运 算 律

由上一节我们看到，定义一个代数结构是很容易的，代数运算也是多种多样的，但不是任何一个都是很有意义的. 我们仅对一些有意义的代数结构感兴趣，这首先要求其运算满足一些重要的运算律，如结合律、交换律和分配律.

1 结合律

定义 $(A,\circ)$为一个代数结构，我们称运算 $\circ$ 满足**结合律**，假若对于任何 $a,b,c\in A$，都有$(a\circ b)\circ c=a\circ(b\circ c)$.

例如，$(\mathbf{C},+)$，$(\mathbf{C},\cdot)$都满足结合律，但$(\mathbf{C},-)$不满足结合律.

对于代数结构$(A,\circ)$中的元素 $a_1,a_2,\cdots,a_n$，通过加括号可使 $a_1\circ a_2\circ\cdots\circ a_n$ 有意义，但从表面上看，不同的方式得到的运算结果可能是 A 中不同的元素. 但是下面的定理告诉我们，对于满足结合律的运算不会发生这种现象，即 $a_1\circ a_2\circ\cdots\circ a_n$ 是有意义的.

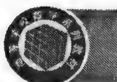
定理 1 若代数结构$(A,\circ)$满足结合律，则对 A 中任何 n $(n\geqslant 3)$ 个元素 $a_1,a_2,\cdots,a_n$，以任何方式加括号得到的有意义的结果都相等.

证明 首先，对于 A 中的元素，我们归纳定义一个标准乘积：

$$\prod_{i=1}^{1}a_i=a_1,\ \prod_{i=1}^{2}a_i=a_1\circ a_2,\cdots,\prod_{i=1}^{n}a_i=\left(\prod_{i=1}^{n-1}a_i\right)\circ a_n.$$

现在我们用 $\pi(a_1\circ a_2\circ\cdots\circ a_n)$ 表示 $a_1\circ a_2\circ\cdots\circ a_n$ 通过加括号得到的一个有意义的结果. 下面我们对元素的个数用归纳法证明此定理.

(1) 当元素的个数是 3 时，由结合律的定义知



$$\pi(a_1 \circ a_2 \circ a_3) = \prod_{i=1}^{3} a_i .$$

(2) 假设元素的个数小于 n 时结论正确,则乘积都等于标准积.

(3) 由归纳假设和加括号的运算过程知

$$\begin{aligned}\pi(a_1 \circ a_2 \circ \cdots \circ a_n) &= (\prod_{i=1}^{m} a_i) \circ (\prod_{i=m+1}^{n} a_i) \\ &= (\prod_{i=1}^{m} a_i) \circ [(\prod_{i=m+1}^{n-1} a_i) \circ a_n] \\ &= [(\prod_{i=1}^{m} a_i) \circ (\prod_{i=m+1}^{n-1} a_i)] \circ a_n \\ &= (\prod_{i=1}^{n-1} a_i) \circ a_n = \prod_{i=1}^{n} a_i \quad (1 \leqslant m < n).\end{aligned}$$

由归纳原理知定理命题成立.

2 交换律

定义 $(A, \circ)$ 为一个代数结构,我们称运算 $\circ$ 满足**交换律**,即假若对于任何 $a, b \in A$,都有 $a \circ b = b \circ a$.

例如,$(\mathbf{C}, +)$,$(\mathbf{C}, \cdot)$ 都满足交换律,但$(\mathbf{C}, -)$ 不满足交换律.

定理 2 若代数结构满$(A, \circ)$足结合律和交换律,则对 A 中任何$n(n \geqslant 2)$个元素 $a_1, a_2, \cdots, a_n$, $a_1 \circ a_2 \circ \cdots \circ a_n$ 中的元素可以任意调换(结果不变).

此定理的证明与上述定理的证明类似,留作练习.

3 分配律

许多有意义的代数结构上有两个代数运算,而且它们是有机结合的,一个运算对另一个有分配律就是一种重要的结合.以下,我们假设 $\otimes$ 是 $B \times A$ 到A 的运算, $\oplus$ 是 A 上的二元运算.

定义 我们称 $\otimes$ 对 $\oplus$ 满足**左分配律**,假若对于任何 $b \in B, a_1, a_2 \in A$,都有

$$b \otimes (a_1 \oplus a_2) = (b \otimes a_1) \oplus (b \otimes a_2).$$

同样我们可定义 $\otimes$ 对 $\oplus$ 满足**右分配律**.

例如,数乘向量满足左分配律;数的乘法对加法满足左分配律和右分配律,而数的减法对加法不满足左分配律和右分配律.

由归纳法我们可以很容易证明如下定理.

定理 3 若 $\oplus$ 满足结合律,而且 $\otimes$ 对 $\oplus$ 满足左分配律,则对于任何 $b \in B, a_1, a_2, \cdots, a_n \in A$ 我们有

$$b \otimes (a_1 \oplus a_2 \oplus \cdots \oplus a_n) = (b \otimes a_1) \oplus (b \otimes a_2) \oplus \cdots \oplus (b \otimes a_n).$$

习题 1 – 3

1.$(\mathbf{R}^*, \div)$ 满足结合律吗?
2.对任意 $a,b \in \mathbf{R}$,定义 $a \circ b = a + 2b$,$(\mathbf{R}, \circ)$ 满足结合律吗?
3.在你已知的非数的运算中找出一个不满足结合律,也不满足交换律的运算.
4.设 $\oplus$ 满足结合律,且 $\otimes$ 对 $\oplus$ 满足左分配律和右分配律,证明

$$(a_1 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_1) \oplus (a_2 \otimes b_2)$$
$$= (a_1 \otimes b_1) \oplus (a_2 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_2)$$

1.4 同态与同构

在代数学中,我们主要关心的是代数结构的抽象运算,而元素用什么表示,运算用何符号无关紧要,因此我们就要建立两个代数结构的比较方法. 我们观察两个极其简单的代数结构 $(A, \cdot)$ 与 $(B, \otimes)$,$A = \{N, Y\}$,$B = \{0,1\}$,运算由下表定义:

$\cdot$	N	Y
N	N	N
Y	N	Y

$\otimes$	0	1
0	0	0
1	0	1

我们自然会说 $(A, \cdot)$ 与 $(B, \otimes)$ 本质上没有什么不同,我们是靠直观做出判断的.但当代数结构很复杂时,如何做出这样的判断? 另一方面,当两个代数结构不完全相同时,我们如何探讨它们某个侧面的相同性?同态与同构就是我们将采取的有效手段.

定义 设 $(A, \circ)$,$(\bar{A}, \bar{\circ})$ 为代数结构,σ 为 A 到 $\bar{A}$ 的映射.

(1) 若对于任何 $a,b \in A$,有 $\sigma(a \circ b) = \sigma(a) \bar{\circ} \sigma(b)$,则我们说 σ 是 A 到 $\bar{A}$ 的**同态**;

(2) 若 σ 是单射同态,我们称 σ 为**单同态**;

(3) 若 σ 是满射同态,我们称 σ 为**满同态**,称 A 与 $\bar{A}$ 同态,记为 $A \geqslant \bar{A}$;

(4) 若 σ 是双射同态,我们称 σ 为**同构**,并称 A 与 $\bar{A}$ 同构,记为 $A \cong \bar{A}$.

(5) 若 σ 是 A 到 A 自身的同态(同构),我们称 σ 为 A 的**自同态(同构)**.

例 1 对于本节开头的两个代数结构 $(A, \cdot)$ 与 $(B, \otimes)$,定义

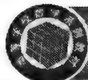
$$\sigma: N \longmapsto 0, Y \longmapsto 1,$$

则 σ 为 A 到 B 的同构.

例 2 对于 $(\mathbf{Z}, +)$ 和 $(U_3, \cdot)$,$\sigma: n \longmapsto \varepsilon_1^n$ 为 $\mathbf{Z}$ 到 U_3 的满同态.

例 3 若令 $\sigma: z \longmapsto \bar{z}$,这里 $\bar{z}$ 为复数 z 的共轭,则 σ 为双射是明显的, 又

$$\sigma(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 = \sigma(z_1) + \sigma(z_2),$$
$$\sigma(z_1 \cdot z_2) = \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2 = \sigma(z_1) \cdot \sigma(z_2),$$



故 σ 为 $(\mathbf{C},\cdot)$ 和 $(\mathbf{C},+)$ 的自同构.

例 4 $\sigma: x \mapsto e^x$ 为代数结构 $(\mathbf{R},+)$ 到 $(\mathbf{R}^+,\cdot)$ 的同构.事实上, σ 为双射是明显的,且

$$\sigma(x_1+x_2)=e^{x_1+x_2}=e^{x_1}e^{x_2}=\sigma(x_1)\cdot\sigma(x_2).$$

定理 假设 $(A,\circ)\geqslant(\bar{A},\bar{\circ})$,则我们有下列结论:

(1) 若 $(A,\circ)$ 满足结合律,则 $(\bar{A},\bar{\circ})$ 也满足结合律;

(2) 若 $(A,\circ)$ 满足交换律,则 $(\bar{A},\bar{\circ})$ 也满足交换律.

证明 我们仅证(1).设 σ 为 A 到 $\bar{A}$ 的满同态.任取 $\bar{a},\bar{b},\bar{c}\in\bar{A}$,由于 σ 为满同态,故存在 $a,b,c\in A$ 使 $\sigma(a)=\bar{a},\sigma(b)=\bar{b},\sigma(c)=\bar{c}$,因而

$$\begin{aligned}(\bar{a}\,\bar{\circ}\,\bar{b})\,\bar{\circ}\,\bar{c}&=(\sigma(a)\,\bar{\circ}\,\sigma(b))\,\bar{\circ}\,\sigma(c)=\sigma(a\circ b)\,\bar{\circ}\,\sigma(c)=\sigma((a\circ b)\circ c)\\&=\sigma(a\circ(b\circ c))=\sigma(a)\,\bar{\circ}\,(\sigma(b\circ c))=\sigma(a)\,\bar{\circ}\,(\sigma(b)\,\bar{\circ}\,\sigma(c))\\&=\bar{a}\,\bar{\circ}\,(\bar{b}\,\bar{\circ}\,\bar{c}),\end{aligned}$$

即 $(\bar{A},\bar{\circ})$ 满足结合律.

习题 1－4

1. 以下映射是不是代数结构 $(\mathbf{R},\cdot)$ 的自同态?

(1) $x\mapsto|x|$; (2) $x\mapsto 2x$; (3) $x\mapsto x^2$; (4) $x\mapsto -x$.

2. 证明 $(A,\circ)\cong(A,\circ)$.

3. 若 $(A,\circ)\geqslant(B,*)$, $(B,*)\geqslant(C,\cdot)$,证明 $(A,\circ)\geqslant(C,\cdot)$.

4. $A=\{a,b,c\}$,其上的运算由下表定义:

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明, $(A,\cdot)$ 满足结合律,且与 1.2 例 5 中的 $(U_3,\cdot)$ 同构.

5. 找 $(\mathbf{Q},+)$ 的一个非恒同的自同构.

6. 在 $\mathbf{R}^2$ 上定义两个二元运算 $\oplus,\otimes$ 使得

$$(\mathbf{R}^2,\oplus)\cong(\mathbf{C},+),\quad(\mathbf{R}^2,\otimes)\cong(\mathbf{C},\cdot).$$

7. 证明 $(\mathbf{Q},+)$ 不与 $(\mathbf{Q}^*,\cdot)$ 同构.

1.5 等价关系与集合的分类

在代数学中除了要比较两个代数结构,当然也要研究一个代数 结构自身的性质.但有时又难以以结构中的元素作为对象直接处理,即我们难以得到此结构中最低层的性质.此时我们

不得不寻找此结构中上层的性质.这样我们要将结构(一个集合)中的元素分类处理,即将一个集合分割成互不相同的子集,以这些子集作为一个新的代数结构中的对象来处理.将一个集合分割成互不相同的子集又与此集合元素间的一个重要关系——等价关系相呼应.

1 等价关系

我们在日常生活中常常谈到各种各样的关系,如"父子关系"、"同事关系"和"同学关系"等.但这些关系如何用数学语言描述呢?我们以"同班同学关系"为例来看.若 S 表示某大学的全部学生,令 $R=\{(s_1,s_2)\in S\times S \mid s_1,s_2$ 在同一个班级中$\}$,则 s_1 与 s_2 有同班同学关系就相当于$(s_1,s_2)\in R$.

定义 $A\times A$ 上的任何一个非空子集 R 称 A 上的一个**关系**.若$(a,b)\in R$,我们称 a 与 b **有 R 关系**,改记为 aRb.

一个集合会有许许多多的关系,但在代数学中我们最关心的是"等价关系"和"偏序关系".本章中我们仅讨论前者.

定义 令 $\sim$ 是集合上的一个关系.若 $\sim$ 满足下列三条,我们则称 $\sim$ 为 A 上的一个**等价关系**:

(Ⅰ)**反身性**:$a\in A\Rightarrow a\sim a$;

(Ⅱ)**对称性**:$a\sim b\Rightarrow b\sim a$;

(Ⅲ)**传递性**:$a\sim b,b\sim c\Rightarrow a\sim c$.

若 $a\sim b$,我们说 a 与 b **等价**.

例1 "等于"关系是等价关系.

例2 若 $\sim$ 为"同班同学关系",则 $\sim$ 是一个学校全体学生之集的等价关系.

2 集合的分类

我们可以将一个学校的全体学生按班级分类,即两个学生在同一个班中等同于这两个学生有同班同学关系.

定义 $p(A)$ 的子集 $\Pi=\{A_i\subset A \mid i\in I\}$ 称集合 A 的一个**分类**,假若 A 中每一个元素属于且只属于 A_i 之一,即下面两项同时成立:

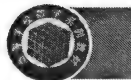
(1)$A=\bigcup\limits_{i\in I}A_i$;

(2)对任何 $i,j\in I$,有 $A_i\cap A_j=\varnothing$ 或 $A_i=A_j$.

例如,一个学校的全体班级是学校全体学生的一个分类,每个学生必在一个班级中,且仅在一个班级中.

定理 集合 A 的一个分类决定 A 的元素间的一个等价关系;反之,A 的元素间的一个等价关系也决定 A 的一个分类.

证明 设 $\Pi=\{A_i\subset A \mid i\in I\}$ 是集合 A 一个分类.定义 A 上的关系 $\sim$:



$$a \sim b \Leftrightarrow a, b \in A_i (\text{对某个 } i \in I).$$

我们说 ~ 是 A 上的等价关系. 事实上,

(Ⅰ) $a \in A = \bigcup_{i \in I} A_i \Rightarrow a, a \in A_i \Rightarrow a \sim a$;

(Ⅱ) $a \sim b \Rightarrow a, b \in A_i \Rightarrow b, a \in A_i \Rightarrow b \sim a$;

(Ⅲ) $a \sim b, b \sim c \Rightarrow a, b \in A_i; b, c \in A_j \Rightarrow b \in A_i \cap A_j \neq \varnothing \Rightarrow a, c \in A_i = A_j \Rightarrow a \sim c$.

反之,设 ~ 是 A 上的等价关系.我们称 A 的子集 $\bar{a} = \{b \in A | b \sim a\}$ 为 a **所代表的等价类**.我们说 $\Pi = \{\bar{a} | a \in A\}$ 是 A 的分类.

等价类的基本性质:

(1) $a \in \bar{a}$;

(2) $a \sim b \Leftrightarrow a \in \bar{b}$;

(3) $a \sim b \Leftrightarrow b \in \bar{a}$;

(4) $a \sim b \Leftrightarrow \bar{a} = \bar{b}$.

证明 (1),(2),(3) 明显成立.我们仅证明(4).

事实上, $\bar{a} = \bar{b} \Rightarrow a \in \bar{a} = \bar{b} \Rightarrow a \sim b$.反之,设 $a \sim b$.此时,

$$c \in \bar{a} \Rightarrow c \sim a, a \sim b \Rightarrow c \sim b \Rightarrow c \in \bar{b} \Rightarrow \bar{a} \subset \bar{b};$$

再由对称性, $\bar{b} \subset \bar{a}$.因此, $a \sim b \Rightarrow \bar{a} = \bar{b}$.

现在,我们推得:

(Ⅰ) $a \in A \Rightarrow a \sim a \Rightarrow a \in \bar{a} \Rightarrow A = \bigcup_{a \in A} \bar{a}$;

(Ⅱ) $\bar{a} \cap \bar{b} \neq \varnothing \Rightarrow$ 存在 $c \in \bar{a}, \bar{b} \Rightarrow c \sim a, c \sim b \Rightarrow a \sim c, c \sim b \Rightarrow a \sim b \Rightarrow \bar{a} = \bar{b}$,

这就证明了 $\Pi = \{\bar{a} | a \in A\}$ 是 A 的分类.

若 ~ 是 A 上的等价关系,我们将它如上决定的分类 $\{\bar{a} | a \in A\}$ 记为 $A/\sim$,称为 A 的**等价类集合**.请记住 $A/\sim \subset p(A)$.

3 整数的同余关系与同余类

现在我们介绍在代数学中重要的整数同余关系与同余类.

同余关系: n 为一个取定的正整数.对于任何 $a, b \in \mathbf{Z}$,我们在 $\mathbf{Z}$ 上定义模 n 的**同余关系** ~:

$$a \sim b \Leftrightarrow n | (a - b).$$

评注:(1) 这里, $p | q$ 表示 p 整除 q; $n | (a - b)$ 等同于 a, b 被 n 除时,余数相同,即"**a 与 b 模 n 同余**"; a 与 b 模 n 同余的通用写法为同余式 $a \equiv b (\mathrm{mod}\, n)$;

(2) 容易证明同余式有下列性质:

① $a \equiv a (\mathrm{mod}\, n)$;

② $a \equiv b (\mathrm{mod}\, n) \Rightarrow b \equiv a (\mathrm{mod}\, n)$;

③ $a \equiv b, b \equiv c (\mathrm{mod}\, n) \Rightarrow a \equiv c (\mathrm{mod}\, n)$;

④ $a \equiv b, c \equiv d (\mathrm{mod}\, n) \Rightarrow a + c \equiv b + d$,

$$ac \equiv bd(\bmod n).$$

上述的 ① ~ ③ 说明同余关系是整数集 **Z** 上的等价关系.

同余类:同余关系决定的等价类称**同余类**.由于任何一个整数被 $n(n>0)$ 除,余数可取为 $0,1,2,\cdots,n-1$ 之一,因而模 n 的一切**同余类集合**为

$$\mathbf{Z}_n = \{\overline{0},\overline{1},\overline{2},\cdots,\overline{n-1}\}.$$

同余类的加法和乘法:在 $\mathbf{Z}_n$ 上,我们定义一个加法 + 和一个乘法 ∘:

$$+:(\overline{a},\overline{b})\longmapsto\overline{a+b}, \text{即 } \overline{a}+\overline{b}=\overline{a+b};$$

$$\circ:(\overline{a},\overline{b})\longmapsto\overline{ab}, \text{即 } \overline{a}\circ\overline{b}=\overline{ab}.$$

评注:在代数中我们经常要在一个等价类集合上定义新的运算,**通过等价类来定义一个二元运算时,必须证实被运算的两个等价类与其代表的选取无关.**

在此我们必须说明 +,∘ 是由 $\mathbf{Z}_n\times\mathbf{Z}_n$ 到 $\mathbf{Z}_n$ 的映射,即下面推理应成立:

$$(\overline{a},\overline{b})=(\overline{c},\overline{d})\Rightarrow\overline{a+b}=\overline{c+d},\quad \overline{a\cdot b}=\overline{c\cdot d}.$$

由于$(\overline{a},\overline{b})=(\overline{c},\overline{d})$相当于 $\overline{a}=\overline{c},\overline{b}=\overline{d}$;但当 $\overline{a}=\overline{c},\overline{b}=\overline{d}$,时,可能有 $a\neq c,b\neq d$,故上述推理不是自然成立的.不过

$$a\equiv c,b\equiv d(\bmod n)\Rightarrow a+b\equiv c+d,\quad a\cdot b\equiv c\cdot d(\bmod n)$$

说明了上述推理成立.总之,以上两个运算是合法的.很显然,$(\mathbf{Z}_n,+)$,$(\mathbf{Z}_n,\circ)$ 满足结合律和交换律,而且乘法 ∘ 对加法 + 满足左分配律和右分配律.

4 同态基本定理

定理 设 σ 为$(A,\circ)$到$(B,\cdot)$的满同态.

(1) 令

$$a_1\sim a_2\Leftrightarrow\sigma(a_1)=\sigma(a_2)(a_1,a_2\in A),$$

则 ~ 为 A 上的等价关系;

(2) 对任意 $\overline{a}_1,\overline{a}_2\in A/\sim$,定义

$$\overline{a}_1\,\overline{\circ}\,\overline{a}_2=\overline{a_1\circ a_2},$$

则$(A/\sim,\overline{\circ})$也是一个代数结构;

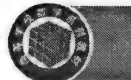
(3) 令 $\overline{\sigma}:A/\sim\rightarrow B,\overline{a}\longmapsto\sigma(a)$,则 $\overline{\sigma}$ 是同构,即 $A/\sim\cong B$.

证明 ~ 为上 A 的等价关系是明显的.由于

$$\begin{aligned}\overline{a}=\overline{b},\overline{c}=\overline{d}&\Rightarrow\sigma(a)=\sigma(b),\sigma(c)=\sigma(d)\\&\Rightarrow\sigma(a)\cdot\sigma(c)=\sigma(b)\cdot\sigma(d)\\&\Rightarrow\sigma(a\circ c)=\sigma(b\circ d)\\&\Rightarrow\overline{a\circ c}=\overline{b\circ d},\end{aligned}$$

故$(A/\sim,\overline{\circ})$为代数结构.

由于 $\overline{a}_1=\overline{a}_2\Leftrightarrow\sigma(a_1)=\sigma(a_2)$,这不仅说明了 $\overline{\sigma}$ 是映射,也说明了 $\overline{\sigma}$ 是单射,$\overline{\sigma}$ 明显是满



射.于是,$\bar{\sigma}$ 为双射;而

$$\bar{\sigma}(\bar{a}\,\bar{\circ}\,\bar{b}) = \bar{\sigma}(\overline{a \circ b}) = \sigma(a \circ b) = \sigma(a)\cdot\sigma(b)$$
$$= \bar{\sigma}(\bar{a})\cdot\bar{\sigma}(\bar{b})$$

又说明 $\bar{\sigma}$ 为同态.因此,$\bar{\sigma}$ 为同构.

例 1 实数集 $\mathbf{R}$ 上的一切 2 阶方阵之集 $M_2(\mathbf{R})$ 对矩阵的乘法构成一个代数结构$(M_2(\mathbf{R}),\cdot)$.令 $\sigma: \boldsymbol{A} \mapsto |\boldsymbol{A}|$,则 σ 为$(M_2(\mathbf{R}),\cdot)$到$(\mathbf{R},\cdot)$的满同态,$|\boldsymbol{AB}| = |\boldsymbol{A}|\cdot|\boldsymbol{B}|$. 由上述定理

$$\boldsymbol{A} \sim \boldsymbol{B} \Leftrightarrow |\boldsymbol{A}| = |\boldsymbol{B}|$$

为 $M_2(\mathbf{R})$ 上的等价关系. 我们容易看到

$$M_2(\mathbf{R})/\sim\ = \left\{\overline{\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix}} \,\middle|\, r \in \mathbf{R}\right\};$$

在运算$\overline{\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix}} \cdot \overline{\begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix}} = \overline{\begin{bmatrix} rs & 0 \\ 0 & 1 \end{bmatrix}}$之下 $M_2(\mathbf{R})/\sim$ 为一个代数结构,且其同构于$(\mathbf{R},\cdot)$.

习题 1－5

1.$\mathbf{R}$ 上的关系 $>$,$\geqslant$ 是不是等价关系?

2.当 $a \neq b$ 时,$\bar{a} \neq \bar{b}$ 是否成立?

3.在$\mathbf{R}^*$ 上定义 $a \sim b \Leftrightarrow a, b$ 的符号相同,此关系是等价关系吗?若是,写出等价类集合$\mathbf{R}^*/\sim$.

4.证明,若 $a \equiv b, c \equiv d \pmod{n}$,则

$$a + c \equiv b + d,\ ac \equiv bd \pmod{n}.$$

5.比较$(\mathbf{Z}_4,\circ)$和$(\mathbf{Z}_5,\circ)$的乘法表,你能发现什么?

6.对于$(\mathbf{Z}_n,+)$,$(\mathbf{Z}_n,\circ)$,求证乘法 $\circ$ 对加法 $+$ 满足左分配律和右分配律.

7.证明,矩阵的等价是 $M_{m\times n}(\mathbf{R})$ 上的等价关系. 对于此等价关系,$M_{m\times n}(\mathbf{R})$ 有多少个等价类.

第 2 章　群　论

有前一章的准备，我们现在来讨论群这个代数结构.群只有一个二元运算，因而我们不再用 $a\circ b$，而将其简写为 ab，称其为 a 与 b 的乘积.现在我们来定义群.

2.1　群的定义

1　群的定义

为后续之便，我们先定义半群.

定义　若代数结构 $(G,\circ)$ 满足结合律，我们称其为**半群**.

例 1　对于任何集合 X，$(p(X),\cup)$ 和 $(p(X),\cap)$ 为**含幺半群**.前者以 $\varnothing$ 为幺：

$$\varnothing\cup A=A\cup\varnothing=A\quad(A\in p(X));$$

后者以 X 为幺：

$$X\cap A=A\cap X=A\quad(A\in p(X)).$$

定义　我们称半群 $(G,\circ)$ 为群，假若它再满足下列条件：

(Ⅰ) G 中有**单位元** e：$ae=ea=a(a\in G)$；

(Ⅱ) G 中每个元 a 都有**逆元** a^{-1}：$aa^{-1}=a^{-1}a=e$.

若群 G 满足交换律，我们称其为**交换群**.

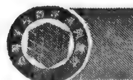
例 2　若 $G=\{e\}$，定义 $ee=e$，则 G 对于这个乘法来说构成一个群.这是最简单的群——**单元群**.

例 3　$(\mathbf{Z},+)$ 是交换群.这里普通的加法就是群中的乘法.此群中的单位元就是 0，a 的逆元是 $-a$.

例 4　$(\mathbf{Q}^*,\cdot)$ 是群；$(\mathbf{Z}^*,\cdot)$ 不是群，尽管它是半群，1 是它的单位元，但除了 ±1 之外，其它元没有逆元.

例 5　$(\mathbf{Z}_n,+)$ 是有 n 个元的交换群，运算为 $\bar a+\bar b=\overline{a+b}$.在第一章中我们已证实这个运算是合法的，其满足结合律是明显的.它的单位元是 $\bar 0$，$\bar a$ 的逆元为 $\overline{-a}$.

例 6　n 为正整数，$U_n=\{z\in\mathbf{C}\mid z^n=1\}$ 为 n 次单位根的集合.我们说 U_n 对复数的乘法构成一个交换群.复数乘法满足结合律，两个单位根的乘积还是单位根；1 是单位元；z 的逆元是 z 的倒数 z^{-1}，单位根的逆元还是单位根.事实上，此群有 n 个元素，若 $\varepsilon=\cos\dfrac{2\pi}{n}+i\sin\dfrac{2\pi}{n}$，



则 $U_n = \{1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{n-1}\}$.

例 7 令 $GL_n(\mathbf{R})(n > 1)$ 为一切实可逆 n 阶方阵之集，由线性代数的知识，我们知道它对矩阵的乘法构成一个非交换群.它的单位元就是 n 阶单位阵 $\boldsymbol{I}$: $\boldsymbol{AI} = \boldsymbol{IA} = \boldsymbol{A}$；每个元 $\boldsymbol{A}$ 的逆元就是它的逆阵 $\boldsymbol{A}^{-1}$: $\boldsymbol{AA}^{-1} = \boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{I}$. $GL_n(\mathbf{R})$ 称为 **n 次一般线性群**.

例 8 令 $W_n = \{(a_1 a_2 \cdots a_n)_2 \mid a_1, a_2, \cdots, a_n = 0 或 1\}$ 为一切 n 位二进位数码，其在异或运算 $\oplus$ 下为群：

$$(a_1 a_2 \cdots a_n)_2 \oplus (b_1 b_2 \cdots b_n)_2 = (c_1 c_2 \cdots c_n)_2,$$
$$c_i \equiv a_i + b_i (\mathrm{mod} 2);$$

$\oplus$ 为 W_n 上的运算明显；其结合律等同于 $(\mathbf{Z}_2, +)$ 的结合律；$(00\cdots0)_2$ 为单位元；每个元明显都有逆元.此群称为**二进位数码词群**.

由上述各例我们看到群是极其广泛的，它们不仅在数学的许多分支，而且在物理，化学，计算机等许多学科也有广泛的应用.

定理 1 若 G 是群，则我们有如下结论：

(1) 单位元唯一；

(2) 消去律成立：

$$ab = ac \Rightarrow b = c(\textbf{左消去律})$$
$$ba = ca \Rightarrow b = c(\textbf{右消去律})$$

(3) 每个元的逆元唯一；

(4) $(a^{-1})^{-1} = a$;

(5) $(ab)^{-1} = b^{-1}a^{-1}$.

证明 (1) 令 e 和 e' 都是单位元，则 $e = ee' = e'$；

(2) $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec \Rightarrow b = c$;
同理可证右消去律；

(3) a_1, a_2 都是 a 的逆元，则 $a_1 a = a_2 a (= e) \Rightarrow a_1 = a_2$;

(4) 明显成立；

(5) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$.

定理 2 设 G 是半群，则 G 是群 $\Leftrightarrow$ 下面(A)，(B)两条成立：

(A) G 中有**左单位元** e: $ea = a(a \in G)$;

(B) G 中每个元 a 都有**左逆元** a^{-1}: $a^{-1}a = e$.

证明 ($\Rightarrow$) 明显成立.

($\Leftarrow$) 此时我们只要证明(Ⅰ)，(Ⅱ)成立.首先我们证实(Ⅱ).任取 $a \in G$，由(B)知，$a^{-1}a = e$.为证 $aa^{-1} = e$，我们先令 $aa^{-1} = c$，再证 $c = e$:

$$cc = (aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = a(ea^{-1}) = aa^{-1} = c,$$
$$cc = c \Rightarrow c^{-1}(cc) = c^{-1}c \Rightarrow (c^{-1}c)c = e \Rightarrow ec = e \Rightarrow c = e.$$

于是，$aa^{-1}=e$，即左逆元也是逆元，(Ⅱ)成立．再由

$$ae=a(a^{-1}a)=(aa^{-1})a=ea=a,$$

我们知左单位元也是单位元，即(Ⅰ)成立．

2　群的阶和元的阶

幂运算：若 a 是群 G 的元，我们约定 a 的幂运算如下：

(1) $a^0=e, a^1=a, a^2=aa, a^3=a^2a,\cdots$;

(2) 若 n 是正整数，$a^{-n}=(a^{-1})^n=(a^n)^{-1}$;

在上述约定下，对任何 $m,n\in\mathbf{Z}$，我们有

$$a^ma^n=a^{m+n};\quad (a^m)^n=a^{mn}.$$

加群：若 G 为交换群，当我们用 + 号表示它的运算时，称它为加群．在加群中，用 0 表示单位元，改称它为零元；用 $-a$ 表示 a 的逆元，并改称它为 a 的负元；用 ma 表示 a 的 m 次幂．

定义　(1) 若群中元的个数有限，称其为**有限群**；否则称其为**无限群**．有限群 G 中元的个数称为此群的**阶**，用 $|G|$ 表示；

(2) a 为群 G 的元．若存在一个使 $a^n=e$ 成立的最小正整数 n，我们称此数为 a 的**阶**，记为 $o(a)$；否则称 a 是**无限阶的**．

评注：(1) 在群中，单位元的阶为 1．

(2) 由于 $a^{-n}=(a^{-1})^n=(a^n)^{-1}$，因而 $a^n=e$ 与 $(a^{-1})^n=e$ 同时成立，从而 $o(a)=o(a^{-1})$．

例 9　在 3 阶群中 $U_3=\{1,\varepsilon_1,\varepsilon_2\}$ 中 $o(1)=1, o(\varepsilon_1)=3, o(\varepsilon_2)=3$，这里

$$\varepsilon_1=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}, \varepsilon_2=\cos\frac{4\pi}{3}+\mathrm{i}\sin\frac{4\pi}{3}.$$

例 10　在 4 阶加群 $\mathbf{Z}_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$ 中，$o(\bar{0})=1, o(\bar{1})=4, o(\bar{2})=2, o(\bar{3})=4$．

例 11　若 p 为素数，求证加群 $\mathbf{Z}_p=\{\bar{0},\bar{1},\cdots,\overline{p-1}\}$ 中除 $\bar{0}$ 外，其它元素的阶都为 p．

证明　首先，当 $0<k<p, 0<l<p$ 时，

$$p\bar{k}=\overbrace{\bar{k}+\cdots+\bar{k}}^{p\text{个}}=\overline{pk}=\bar{0};$$

$$p\nmid kl\Rightarrow l\bar{k}=\overbrace{\bar{k}+\cdots+\bar{k}}^{l\text{个}}=\overline{lk}\neq\bar{0}.$$

总之，p 是使 $p\bar{k}=\bar{0}$ 的最小正整数，故 $o(\bar{k})=p$．

习题 2－1

1．集合 $A=\{1,2\}$ 上的一切变换 T_A 在映射的复合运算下是含幺半群吗？它是群吗？

2．若群 G 中的每个元都满足方程 $x^2=e$，那么 G 是交换群．

3．在一个有限群中，阶大于 2 的元的个数一定是偶数．

4．若 $|G|=2k$，则群 G 中阶是 2 的元的个数一定是奇数．

5. 有限群的每个元的阶都有限.

6. 找出加群 $\mathbf{Z}_6$ 中每个元的阶.

7. 在群 G 中,元 a 的阶为 $n \Leftrightarrow a^n = e(n \geqslant 1)$,且当 $a^m = e(m \geqslant 1)$ 时,有 $n|m$.

8. 令 $G = \mathbf{Z} \times \mathbf{Z}_2$,对任何 $(a,\bar{b}),(c,\bar{d}) \in G$,定义

$$(a,\bar{b}) + (c,\bar{d}) = (a + c,\bar{b} + \bar{d}).$$

证明 $(G, +)$ 为加群.它的零元是什么?此群是有限群吗?此群中有有限阶且不是零元的元吗?此群中有阶无限的元吗?

9. 设 G 是半群.证明,G 是群 $\Leftrightarrow$ 下面(C)成立:

(C) 对任何 $a,b \in G$,方程 $ax = b, ya = b$ 在 G 中有解.*

10. 若半群 G 中元素的个数有限,且左消去律和右消去律成立,则 G 是群.*

2.2 群的同态与变换群

1 群的同态

群作为一种特殊的代数结构,其同态也有其特殊性.

定理 1 设 σ 是群 G 到群 G' 的同态(不必为满同态),则我们有下列结论:

(1) 若 e 是 G 的单位元,则 $\sigma(e)$ 是 G' 的单位元;

(2) 对任何 $a \in G$,在 G' 中 $\sigma(a^{-1})$ 为 $\sigma(a)$ 的逆元,即有

$$\sigma(a^{-1}) = \sigma(a)^{-1}.$$

证明 (1) 设 e' 为 G' 的单位元,则

$$\sigma(e)\sigma(e) = \sigma(ee) = \sigma(e)e',$$

再由左消去律,我们得到 $\sigma(e) = e'$.

(2) 由于

$$\sigma(a^{-1})\sigma(a) = \sigma(a^{-1}a) = \sigma(e),$$
$$\sigma(a)\sigma(a^{-1}) = \sigma(aa^{-1}) = \sigma(e),$$

故 $\sigma(a^{-1})$ 是 $\sigma(a)$ 的逆元.

定义 若 $\sigma: G \to G'$ 为群同态,e' 为 G' 的单位元,我们称

$$\ker\sigma = \sigma^{-1}(e') = \{a \in G | \sigma(a) = e'\}$$

为同态 σ 的核.

定理 2 若 $\sigma: G \to G'$ 为群同态,则 σ 为单同态 $\Leftrightarrow \ker\sigma = \{e\}$.

证明 $(\Rightarrow)$ 令 σ 为单同态. 此时,任取 $a \in \ker\sigma$,由定理 1 我们有 $\sigma(a) = e' = \sigma(e)$.再由 σ 的单性,有 $a = e$,即 $\ker\sigma = \{e\}$.

$(\Leftarrow)$ 反之,令 $\ker\sigma = \{e\}$. 我们有

$$\sigma(a)=\sigma(b)\Rightarrow\sigma(b^{-1})\sigma(a)=e'\Rightarrow\sigma(b^{-1}a)=e'$$
$$\Rightarrow b^{-1}a\in\ker\sigma\Rightarrow b^{-1}a=e\Rightarrow a=b$$

即 σ 为单同态.

2 变换群

代数学的本质是抽象的，但我们不是为了抽象而抽象.对于抽象的对象我们还是尽力给它一个具体的表示，这是现代代数学的很重要的一个方面.变换群就是群的一种具体的表示.

定理 3 集合 A 上的一切变换之集 T_A 对于映射的复合构成一个含幺半群.

评注：由于变换 $\alpha:A\to A$ 为一一变换的充要条件为存在 $\beta:A\to A$ 使得 $\alpha\beta=\beta\alpha=1_A$，故 A 的若干变换对映射的复合要构成群，则此群必含有 1_A，而且其中的每个变换必为一一变换.

定义 由 A 的若干(不一定是全部)一一变换构成的群称为 A 的(一个) **变换群**.

定理 4 集合 A 上的一切一一变换之集构成 A 的一个变换群 S_A，称其为 A 上的**对称群**.

例 2 $A=\{1,2\}$ 上的一切一一变换为

$$\alpha:1\mapsto 1,2\mapsto 2;\quad \beta:1\mapsto 2,2\mapsto 1;$$

$S_2=\{\alpha,\beta\}$ 为 A 上最大的变换群.

定理 5 任何一个群 G 都同构其自身的一个变换群.

证明 我们先造出这个变换群，再证明 G 与其同构.对任何 $g\in G$，造 G 上的**左平移** L_g 如下：

$$L_g:x\mapsto gx(x\in G).$$

令 $L_G=\{L_g|g\in G\}$，则它是与 G 同构(G 上)的变换群.由

$$(L_gL_h)(x)=L_g(L_h(x))=L_g(hx)=g(hx)$$
$$=(gh)(x)=L_{gh}(x),$$

我们得到下面的结论：

(1) 运算封闭：$L_gL_h=L_{gh}\in L_G$.

(2) 满足结合律：$(L_gL_h)L_k=L_g(L_hL_k)=L_{ghk}$.

(3) 有单位元 L_e：$L_eL_g=L_gL_e=L_g$.

(4) L_g 有逆元 $L_{g^{-1}}$：$L_{g^{-1}}L_g=L_gL_{g^{-1}}=L_e$.

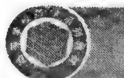
令 $\sigma:g\mapsto L_g$，则 σ 明显是由 G 到 L_G 的满射.下面的运算说明 σ 是单射和同态，进而，是同构：

$$\sigma(g)=\sigma(h)\Rightarrow L_g=L_h\Rightarrow L_g(e)=L_h(e)\Rightarrow g=h,$$
$$\sigma(gh)=L_{gh}=L_gL_h=\sigma(g)\sigma(h).$$

上述定理说明任何一个抽象的群都可在变换群中找到一个具体的实现.

习题 2－2

1.假设群 G 与群 $\bar{G}$ 同态，同态为 σ. 对任意 $a\in G$，a 与 $\sigma(a)$ 的阶是否相同?



2.群$(\mathbf{Z}_4, +)$是否与$(\mathbf{Z}_2, +)$同态?

3.群$(\mathbf{Z}, +)$是否与$(\mathbf{Z}_n, +)$同态?

4.$a,b\in\mathbf{Q}, a\neq 0$,令$l_{a,b}: x\longmapsto ax+b(x\in\mathbf{R})$. 证明,一切$l_{a,b}$之集$L$是$\mathbf{R}$的一个变换群.此群是交换群吗?

5.证明在平面内环绕一个定点的一切旋转构成此平面的一个变换群.此群是交换群吗?

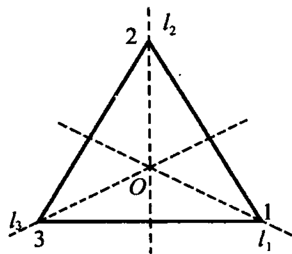


图 2-1

6.如图2-1,令R是正三角形绕中心O逆时针旋转120°,R^2是正三角形绕O逆时针旋转240°;T_1是正三角形关于对称轴l_1的翻转,T_2是正三角形关于对称轴l_2的翻转,T_3是正三角形关于对称轴l_3的翻转.证明,这些变换加上恒同变换I构成的集合D_3(有6个元)是此正三角形的一个变换群.写出此群的乘法表.

2.3 置 换 群

1 置换群

有限集的变换群称置换群,在代数学中占有很重要的地位.这不仅是因为每个有限群都同构于一个置换群,而且在历史上,群论的创始人,法国天才少年数学家伽罗瓦(Galois, 1811—1832)就是开创性地研究了置换群,从而证明了当$n\geqslant 5$时,一元n次方程不能用根式解(没有用根式表示的公式解)的世纪难题.这种群的元素可用很具体的符号表示,运算直观.

n 元置换:集合$\{1,2,3,\cdots,n\}$的一一变换.

n 元置换群:若干n元置换构成的群.

n 次对称群 S_n:一切n元置换构成的群.

定理 1 S_n的阶为$n!$.

我们将n元置换记为$\sigma: 1\longmapsto k_1, 2\longmapsto k_2,\cdots,n\longmapsto k_n$记为

$$\begin{pmatrix}1 & 2 & \cdots & n\\ k_1 & k_2 & \cdots & k_n\end{pmatrix}.$$

例 1 用上面的符号,S_3的全部6个元素如下:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

我们将看到,6阶以下的群都是交换群.S_3是元素最少的非交换群.例如,

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$
$$\neq\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

2 置换的循环表示

尽管上面的表示很直观，但还是不方便．下面我们用循环来表示一个置换．

k - 循环：若置换 $\sigma\in S_n:i_1\mapsto i_2\mapsto\cdots\mapsto i_k\mapsto i_1$，且 σ 保持其它的 $n-k$ 个数字不动，我们称 σ 为一个 **k - 循环**；我们将它记为 $(i_1 i_2\cdots i_k)$，$(i_2 i_3\cdots i_k i_1)$ 等．

对换：我们称 2 - 循环为**对换**．

不相交循环：若两个循环中没有相同的数字，我们称它们是**不相交的**．不相交的两个循环的乘积明显是可交换的．

例 2 在 S_5 中，

$$\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}=(1),\quad\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}=(34),$$
$$\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}=(123),\quad\begin{pmatrix}1&2&3&4&5\\4&1&2&3&5\end{pmatrix}=(4321);$$

但不是每个置换都是循环．例如，

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=(123)(45)=(45)(123)$$

不是循环，但却可以写成不相交循环的乘积．

定理 2 任何 n 元置换 σ 都可分解成若干个不相交循环的乘积．若要求 1 到 n 每个数字在这些循环中出现且仅出现一次，且不记次序，则这种分解是唯一的．

证明 任取 $i_1\in\{1,2,3,\cdots,n\}$．数字列

$$i_1,\sigma(i_1),\sigma^2(i_1),\sigma^3(i_1),\cdots$$

中必有重复数字．设第一个与前面重复的是 $\sigma^k(i_1)$．我们说 $\sigma^k(i_1)=i_1$．事实上，若 $\sigma^k(i_1)=\sigma^l(i_1)$，$0<l<k$，则 $\sigma^{k-l}(i_1)=i_1$，$0<k-l<k$，这同 $\sigma^k(i_1)$ 的身份矛盾．令

$$i_2=\sigma(i_1),i_3=\sigma^2(i_1),\cdots,i_k=\sigma^{k-1}(i_1),$$

则

$$\sigma_1=(i_1 i_2\cdots i_k)$$

是一个 k - 循环．再取 $j_1\in\{1,2,\cdots,n\}-\{i_1,\cdots,i_k\}$，同样我们可得到另一个 l - 循环

$$\sigma_2=(j_1 j_2\cdots j_l),$$

这两个循环明显是不相交的．这样继续下去，直到用完 $\{1,2,3,\cdots,n\}$ 中的每个数字，我们得到一串不相交的循环 $\sigma_1,\sigma_2,\cdots,\sigma_m$，且 1 到 n 中每个数字出现且仅出现在这些循环中的一个中．

此时通过检验 σ 和 $\sigma_1\sigma_2\cdots\sigma_m$ 在每个数字上的作用,我们知

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m.$$

因为不相交的循环可交换,因而不记次序后,分解唯一.

例 3 S_4 的全部 24 个元用循环表示为:

(1);

(12),(34),(13),(24),(14),(23);

(123),(132),(134),(143),(124),(142),(234),(243);

(1234),(1243),(1324),(1342),(1423),(1432);

(12)(34),(13)(24),(14)(23).

3 置换的奇偶性

由于每个循环都可写成若干对换的乘积:

$$(i_1 i_2\cdots i_k) = (i_1 i_k)\cdots(i_1 i_3)(i_1 i_2), \quad (i) = (i\,j)(i\,j).$$

例如,(1234) = (14)(13)(12),(1) = (12)(12).再由上述定理 2,我们得知每个置换都可分解成若干个对换的乘积,尽管这种分解不是唯一的,例如(1) = (12)(12) = (12)(12)(23)(23),但有一个重要的不变性,即所用对换的个数的奇偶性不变.

定理 3 每个置换 σ 都可分解成若干对换的乘积,且所用对换的个数的奇偶性不变.

证明 首先,我们对每个置换标记上一个确定的自然数,即建立一个由 S_n 到 $\mathbf{N}$ 的映射 Δ.若

$$\sigma = (i_1 i_2\cdots i_r)(j_1 j_2\cdots j_s)\cdots(l_1 l_2\cdots l_u)$$

是 σ 满足定理 2 的唯一分解,令

$$\Delta(\sigma) = (r-1)+(s-1)+\cdots+(u-1).$$

我们将证明,对于任何对换(ab)必有

$$\Delta(\sigma(ab)) = \Delta(\sigma)\pm 1.$$

(1)a,b 出现在σ 的同一个循环因子$(ac_1\cdots c_h b d_1\cdots d_k)$中. 此时,由公式

$$(ac_1\cdots c_h b d_1\cdots d_k)(ab) = (ad_1\cdots d_k)(bc_1\cdots c_h),$$

{例如,(123456)(14) = (156)(423)}

知 $\Delta(\sigma(ab)) = \Delta(\sigma)-1$;

(2)a,b 出现在σ 的不同的两个循环因子$(ac_1\cdots c_h)$和$(bd_1\cdots d_k)$中.此时,由公式

$$(ac_1\cdots c_h)(bd_1\cdots d_k)(ab) = (ad_1\cdots d_k bc_1\cdots c_h),$$

{例如,(123)(456)(14) = (156423)}

知 $\Delta(\sigma(ab)) = \Delta(\sigma)+1$.

现在,假设 $\sigma = (a_1 b_1)(a_2 b_2)\cdots(a_m b_m)$.由于$(i\,j)^{-1} = (i\,j)$,故 $\sigma(a_m b_m)\cdots(a_2 b_2)(a_1 b_1) = (1)$.重复利用 $\Delta(\sigma(ab)) = \Delta(\sigma)\pm 1$,我们得到

$$\Delta(\sigma)\pm 1\pm\cdots\pm 1 = \Delta(\sigma(a_m b_m)\cdots(a_2 b_2)(a_1 b_1))$$

$$= \Delta((1)) = 0(m\text{ 个 }\pm 1),$$

这说明 m 与 $\Delta(\sigma)$ 有相同的奇偶性，而 $\Delta(\sigma)$ 由 σ 唯一决定，因而定理命题成立.

奇置换和偶置换：若 σ 能分解成奇数个对换的乘积，我们称其为**奇置换**，否则称其为**偶置换**.

例 4 当 $n \geqslant 2$ 时，S_n 的一切偶置换之集 A_n 构成一个置换群，这由下面的四项可以看出：

(1) 偶置换与偶置换的乘积还是偶置换；

(2) 结合律是天然的；

(3) $(1) = (12)(12)$，单位元是偶置换；

(4) 偶置换的逆元还是偶置换.

我们称此群为 n **次交错群**，它的阶为 $\frac{1}{2}n!$. 历史上，伽罗瓦深入地研究了群 A_n，证实了当 $n \geqslant 5$ 时，A_n 有一种特性，从而证实了他的结论（本节开头所述）.

习题 2 - 3

1. 将 S_3 中的元分解成不相交循环的乘积，并写出 S_3 的乘法表.
2. 找出 S_3 中与 (123) 交换的元.
3. 证明 $(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$.
4. 证明 k - 循环的阶是 k.
5. 证明 S_n 的元都可写成 $(12),(13),\cdots,(1n)$ 中若干个的乘积. *

2.4 循环群和两面体群

上两节告诉我们，若把变换群完全研究清楚，那就等于把一切群都研究清楚了；如果我们把置换群完全研究清楚了，也就把一切有限群研究清楚了. 但事实告诉我们，研究变换群不比直接研究抽象群容易，直接方法研究抽象群还是非常重要的.

研究群的最终目的是把所有的抽象群都找出来，就是看一看，一共有多少个互不同构的群. 为此，企图一下子把所有的群都找出来几乎是不可能的. 一般方法是把群分成若干类，比如，有限群，交换群等，然后看一看，每一类有多少不同的群. 不过，到现在为止，我们对群的认识还很有限，完全弄清楚的群只有少数几类. 尽管如此，群在实践上和理论上还是有其广泛和重要应用. 在本节中，我们介绍两类应用最广泛的群 —— 循环群和两面体群.

1 循环群

定义 若群 G 中的每个元都是某个固定元 a 的幂，我们就称 G 为**循环群**，称 a 为它的**生成元**，并记为 $G = (a)$.

例 1 整数加群 **Z** 是无限循环群. 事实上，若 $m > 0$，有

$$m = 1 + 1 + \cdots + 1 = m1 = (-m)(-1);$$
$$-m = (-1) + (-1) + \cdots + (-1) = (-m)1 = m(-1),$$
$$0 = 01 = 0(-1),$$

故 $\mathbf{Z} = (1) = (-1)$.由此,我们也看到,循环群的生成元一般不唯一.

例 2 $\mathbf{Z}$ 模 n 的同余类加群 $\mathbf{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ 是有限循环群.由于 $\bar{k} = k\bar{1}$,故 $\mathbf{Z}_n = (\bar{1})$.事实上,若 d 与 n 互素,则 $\mathbf{Z}_n = (\bar{d})$.

例 3 n 次单位根的乘法群 U_n 是循环群.事实上,若 $\varepsilon = e^{\frac{2\pi}{n}i}$,则 $U_n = (\varepsilon)$.

我们说,通过循环群 $\mathbf{Z}$ 和 $\mathbf{Z}_n$,我们就知道了一切循环群,因为我们有下面的定理.

定理 设 $G = (a)$ 为循环群,那么我们有如下结论:

(1) 若 a 的阶无限,则 $G \cong \mathbf{Z}$,且
$$G = \{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \cdots\};$$

(2) 若 a 的阶为 n,则 $G \cong \mathbf{Z}_n$,且
$$G = \{e, a^1, a^2, \cdots, a^{n-1}\}.$$

证明 (1) 设 a 的阶无限.此时,我们断言
$$a^h = a^k \Leftrightarrow h = k.$$
若 $h = k$,自然有 $a^h = a^k$.假若 $a^h = a^k$,而 $h \neq k$.不妨设 $h > k$,则由 $a^h = a^k$ 得到 $a^{h-k} = e$,这同 a 的阶无限矛盾.这样,$\sigma: a^k \mapsto k$ 是 G 到 $\mathbf{Z}$ 的双射;又
$$\sigma(a^h a^k) = \sigma(a^{h+k}) = h + k = \sigma(a^h) + \sigma(a^k),$$
所以 $G \cong \mathbf{Z}$.

(2) 设 a 的阶为 n.此时,我们有
$$a^h = a^k \Leftrightarrow n \mid (h - k) \Leftrightarrow \bar{h} = \bar{k}.$$
事实上,
$$n \mid (h - k) \Rightarrow h - k = nq \Rightarrow h = k + nq \Rightarrow a^h = a^{k+nq} = a^k a^{nq} = a^k (a^n)^q = a^k;$$
反之,令 $h - k = nq + r, 0 \leqslant r < n$.若
$$a^h = a^k \Rightarrow e = a^{h-k} = a^{nq+r} = a^{nq} a^r = a^r,$$
则必有 $r = 0$,否则将有一个比 n 小的正整数 r 使 $a^r = e$,这同 n 是 a 的阶矛盾.现在,令 $\sigma: a^k \mapsto \bar{k}$,则 σ 是双射;又
$$\sigma(a^h a^k) = \sigma(a^{h+k}) = \overline{h + k} = \bar{h} + \bar{k} = \sigma(a^h) + \sigma(a^k),$$
所以 $G \cong \mathbf{Z}_n$.

到此,我们就彻底掌握了一切循环群.在代数学中,对一类代数结构,我们就是要解决它们的存在性,数量问题和构造问题.如果我们能得到循环群那样的结果,那么我们的目的就算达到了.

2 两面体群

图形的对称:令 F 为空间(平面或立体)图形.由 F 到 F 自身的保距双射 σ 称此图形的**对称**

（变换），即 $\sigma:F\to F$ 为双射，且对任何 $a,b\in F$，a 与 b 的距离等于 $\sigma(a)$ 与 $\sigma(b)$ 的距离．

对称群：空间一个图形的一切对称在映射的复合运算下构成此图形的一个变换群，我们称其为此图形的**对称群**．

例 4　写出长宽不等长方形对称群的运算表．

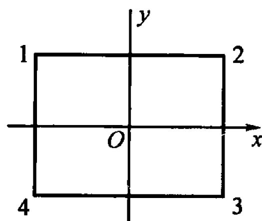


图 2－2

解　见图 2－2，长方形的对称有四个：

恒同 e；

绕 x 轴的翻转 a；

绕 y 轴的翻转 b；

绕中心 O 旋转 180° 的 c．

此群 $K=\{e,a,b,c\}$ 的运算表如下：

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

此群称为 Klein 四元群，它为交换群（见习题 2－5－11）．

例 5　正 n 边形的对称群称为**两面体群**，记为 D_n．下面我们讨论 D_n 中元素的表示．

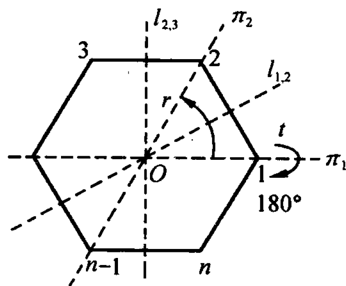


图 2－3

正 n 边形的对称分两类：绕中心的 n 个旋转和绕 n 个对称轴 180° 的翻转，因而 D_n 的阶为 $2n$．

如图 2－3，令 r 是以 O 为心，在平面内的 $\frac{2\pi}{n}$ 弧度的逆时针方向旋转，则

$$r=\begin{pmatrix}1&2&\cdots&n\\2&3&\cdots&1\end{pmatrix},$$

$$o(r)=n,$$

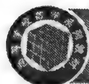
且 n 个旋转为：$e=r^0,r,r^2,\cdots,r^{n-1}$．令 t 为绕对称轴 π_1 的 180° 翻转，则

$$t=\begin{pmatrix}1&2&3&\cdots&n-1&n\\1&n&n-1&\cdots&3&2\end{pmatrix},\quad o(t)=2,$$

n 个翻转为：$t,rt,r^2t,\cdots,r^{n-1}t$；例如，

$$rt=\begin{pmatrix}1&2&3&\cdots&n-1&n\\2&1&n&\cdots&4&3\end{pmatrix}$$

为绕对称轴 $l_{1,2}$ 的翻转．通过计算我们可以验证：$r^kt=tr^{n-k}$（为方便计算，最好用 $\mathbf{Z}$ 模 n 的同



余类 $\bar{1},\bar{2},\cdots,\bar{n}$ 表示正 n 边形的顶点）. 总之，

$$D_n = \{e, r, r^2, \cdots, r^{n-1}, t, rt, r^2t, \cdots, r^{n-1}t\}.$$

习题 2－4

1. 证明循环群是交换群.
2. 设 $G = (a)$ 为 n 阶循环群. 若 r 与 n 互素，则 $G = (a^r)$.
3. 若 $o(a) = n, r > 0$，则 $o(a^r) = \dfrac{n}{d}$，这里 $d = (r, n)$.
4. 设 $G \geqslant \bar{G}$，且 G 是循环群. 证明 $\bar{G}$ 也是循环群.
5. 设 G 是无限循环群，$\bar{G}$ 是任何循环群. 证明 G 与 $\bar{G}$ 同态.
6. 用正三角形顶点的置换表示 D_3 的元素，并证明 $D_3 \cong S_3$.
7. 用例 4 的符号写出两面体群 D_4 的运算表.

2.5　子群与子群的陪集

在群论中，如循环群那样彻底解决的群只有少数几种. 限于本课程的范围，我们不再一一介绍了. 我们还是要介绍研讨抽象群的一般方法，如利用一个群的特殊子集来推测整个群的性质. 子群和正规子群是我们将要讨论的两种群的特殊子集.

1　子群

定义　H 是群 G 的子集. 若 H 对于 G 的乘法也构成一个群，则我们称 H 是 G 的一个子群，记为 $H \leqslant G$.

例 1　任何一个群 G 至少有两个**平凡子群**，G 和 $\{e\}$.

用定义直接判别一个群的子集是子群很不方便，下面我们给出更好的方法.

定理 1　设 H 是群 G 的子集，则以下三项是等价的：

(1) $H \leqslant G$;

(2) $a, b \in H \Rightarrow ab \in H$;　$c \in H \Rightarrow c^{-1} \in H$;

(3) $a, b \in H \Rightarrow ab^{-1} \in H$.

证明　(1)$\Rightarrow$(2) 明显成立；

(2)$\Rightarrow$(3)　$a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow ab^{-1} \in H$;

(3)$\Rightarrow$(1) 我们用子群的定义来证明 $H \leqslant G$:

① $a, a \in H \Rightarrow e = aa^{-1} \in H$;

② $e, a \in H \Rightarrow a^{-1} = ea^{-1} \in H$;

③ $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow ab = a(b^{-1})^{-1} \in H$;

④H 自然有结合律.

以上我们看到 H 对于 G 的乘法封闭.由于 G 的单位元 e 在 H 中,只要 H 运算封闭,e 自然是 H 的单位元;又若 $a \in H$,则它在 G 中的逆元 $a^{-1} \in H$,同样,只要 H 运算封闭,a^{-1} 自然也是 a 在 H 中的逆元.总之,$H \leqslant G$.

例 2 $G = S_3, H = \{(1),(12)\}$,则 $H \leqslant G$.由定理 1,这是明显的.

例 3 若 $\sigma: G \to G'$ 为群同态,则 σ 的核 $\ker\sigma$ 为 G 的子群.事实上,

$$\sigma(e) = e' \Rightarrow e \in \ker\sigma \Rightarrow \ker\sigma \neq \varnothing;$$

$$a,b \in \ker\sigma \Rightarrow \sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)\sigma(b)^{-1} = e'e'^{-1} = e'$$
$$\Rightarrow ab^{-1} \in \ker\sigma.$$

2 生成子群

要找一个群 G 的一个子群,一般我们先选 G 的一个子集 S,如 $S = \{a,b\}$.当然 S 未必是子群,但我们可试着将其扩大成一个子群,扩大成 G 当然没意思,有意思的是我们要做最小的扩大,找含 S 的最小的子群.

定义 S 是群 G 的子集,我们用 (S) 表示 G 中包含 S 的最小的子群,即若 $S \subset H \leqslant G$,则 $(S) \subset H$. 我们称 (S) 为 S 生成的**生成子群**.

例如,循环群 $G = (a)$ 就是其生成元 a 的生成子群.

为了猜猜 (S) 到底是什么样,我们以 $S = \{a,b\}$ 为例.由子群的定义,下列形式的乘积都应在 (S) 中:

$$a^{-1}a, ab, a^2b, a^{-3}b^2, ba^2b, a^2ba^{-1}b, aba^2ba, \cdots.$$

当然上面的序列可能是无限项,也可能是有限项,这是因为在某些条件下,例如 $ab^2 = e$ 等,它们可能会简化,两个乘积可能相等.事实上,(S) 就是由 S 中的元素,按如上的方式得到的一切乘积.在习题中有 (S) 的其它描述方式.

3 子群的陪集

有了一个子群后,我们最想做的就是参照这个子群来研究原来的群.首先我们可参照一个子群将原来的群中的元素分类.为此我们先从另一个角度看整数加群 $\mathbf{Z}$ 的模 n 的同余类加群 $\mathbf{Z}_n$.

若 $n\mathbf{Z} = \{0, \pm n, \pm 2n, \pm 3n, \cdots\}$,很明显 $n\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个子群.若 ~ 是模 n 的同余关系,则

$$a \sim b \Leftrightarrow n \mid (a-b) \Leftrightarrow a - b = pn \Leftrightarrow a - b \in n\mathbf{Z},$$

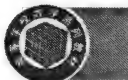
而 $\mathbf{Z}_n$ 就是模 n 的同余关系决定的等价类之集.

事实上,若 $H \leqslant G$,定义 $a \sim b \Leftrightarrow ab^{-1} \in H$,则 ~ 是 G 上的一个等价关系:

(1) 反身性:$aa^{-1} = e \in H \Rightarrow a \sim a$;

(2) 对称性:$a \sim b \Rightarrow ab^{-1} \in H \Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H \Rightarrow b \sim a$;

(3) 传递性:$a \sim b, b \sim c \Rightarrow ab^{-1}, bc^{-1} \in H \Rightarrow ac^{-1} = (ab^{-1})(bc^{-1}) \in H \Rightarrow a \sim c$.



子集的乘积：H,K 是群 G 的两个子集，我们定义

$$HK \equiv \{hk \mid h \in H, k \in K\};$$

同样我们可定义多个集合的乘积.

子群的陪集：若 $H \leqslant G, a \in G$，我们称

$$Ha = \{ha \mid h \in H\}, \quad aH = \{ah \mid h \in H\}$$

分别为 H 的一个**右陪集**和一个**左陪集**；它们都是 G 的子集.

~ 的等价类：~ 如上定义，则 $a \in G$ 所在的等价类 $\bar{a} = Ha$.

事实上，

$$b \in \bar{a} \Leftrightarrow b \sim a \Leftrightarrow ba^{-1} = h \in H \Leftrightarrow b = ha \in Ha.$$

若定义 $a \approx b \Leftrightarrow b^{-1}a \in H$，同样我们可证实 $\approx$ 也是 G 上的一个等价关系. 此时，$a \in G$ 所在的等价类 $\bar{a} = aH$.

总之，请记住下面的结论：

$$Ha = Hb \Leftrightarrow ab^{-1} \in H;$$
$$aH = bH \Leftrightarrow b^{-1}a \in H;$$
$$a \in H \Leftrightarrow aH = Ha = H.$$

例 4 $S_3 = \{(1),(12),(13),(23),(123),(132)\}$，$H = \{(1),(12)\}$，则

$$H(1) = \{(1),(12)\}, \qquad H(13) = \{(13),(132)\},$$
$$H(23) = \{(23),(123)\}, \qquad H(12) = H(1),$$
$$H(132) = H(13), \qquad H(123) = H(23);$$
$$(1)H = \{(1),(12)\}, \qquad (13)H = \{(13),(123)\},$$
$$(23)H = \{(23,(132)\}; \qquad (12)H = H(1),$$
$$(132)H = (23)H, \qquad (123)H = (13)H.$$

定理 2 设 H 是 G 群的子群，令

$$S_R \equiv \{Ha \mid a \in G\}, \quad S_L \equiv \{aH \mid a \in G\},$$

则我们有下面的结论：

(1) S_R 与 S_L 一一对应；

(2) Ha, aH 与 H 一一对应.

证明 (1) 由于

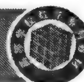
$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (ab^{-1})^{-1} = ba^{-1} = (b^{-1})^{-1}a^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H,$$

故 $\alpha: Ha \longmapsto a^{-1}H$ 是 S_R 到 S_L 的一一对应.

(2) 由于消去律在群中成立，故 $\beta: ha \longmapsto h$ 是 Ha 到 H 的一一对应.

定义 H 是群 G 的子群，H 在 G 中右陪集(或左陪集)的个数称为 H 在 G 中的**指数**，记为 $[G:H]$.

由定理 2，我们可得到下面这个极其重要的定理.



定理 3 设 H 是有限群 G 的子群,则

$$|G| = [G:H]\cdot|H|;$$

特别是,$|H|$ 和 $[G:H]$ 都 $|G|$ 的因子.

推论 若 G 是有限群,$a\in G$,则 a 的阶整除 G 的阶.

证明 a 生成 G 的一个子群 (a),其阶就是元 a 的阶,再由定理 3 得到此推论.

例 5 n 次交错群 A_n 是 n 次对称群 S_n 的子群.若 α 为偶置换,则 $\alpha\in A_n$,从而 $\sigma A_n = A_n = (1)A_n$;若 α 为奇置换,则 $(12)^{-1}\alpha$ 为偶置换,$(12)^{-1}\alpha\in A_n$,从而 $\alpha A_n = (12)A_n$.总之,$[S_n:A_n]=2$.

习题 2 - 5

1. 找出 S_3 的所有子群.
2. 证明,群 G 的任意个子群的交也是 G 的子群,从而证明 S 在 G 中的生成子群 (S) 是 G 中包含 S 的一切子群的交.
3. 取 S_3 的子集 $S=\{(12),(123)\}$,$(S)=$?一个群的两个不同的集会生成相同的子群吗?
4. 两面体群 D_n 最少可由多少元素生成.
5. 证明循环群的子群还是循环群.
6. 找出 $\mathbf{Z}_{12}$ 的所有子群.
7. 证明阶是素数的群是循环群.
8. 证明阶是 p^m(p 是素数)的群一定包含一个阶是 p 的子群.
9. 假定 a,b 是群 G 的两个元,$ab=ba$,$(o(a),o(b))=1$.证明

$$o(ab)=o(a)\cdot o(b).$$

10. 令 $H\leqslant G$,$a,b\in G$.直接证明

$$Ha=Hb\Leftrightarrow ab^{-1}\in H,\quad aH=bH\Leftrightarrow b^{-1}a\in H.$$

11. 若同构的群视为相同,证明阶为 4 的群仅有两个 —— 循环群和 Klein 四元群.*
12. 设 H 是群 G 的一个非空有限子集,求证 $H<G\Leftrightarrow H$ 的运算封闭.*
13. 设 H,K 是 G 群的两个有限子群:

(1) 对任意 $(h_1,k_1),(h_2,k_2)\in H\times K$,定义

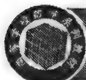
$$(h_1,k_1)\sim(h_2,k_2)\Leftrightarrow h_1k_1=h_2k_2,$$

求证 $\sim$ 为集合 $H\times K$ 上的一个等价关系;

(2) 证明 $|H|\cdot|K|=|HK|\cdot|H\cap K|$.*

2.6 正规子群与商群

在上一节中我们看到子群 $n\mathbf{Z}$ 在 $\mathbf{Z}$ 中的左陪集的集合为 $\mathbf{Z}_n$,a 所在的左陪集 $a+n\mathbf{Z}=\bar{a}$,而在 $\mathbf{Z}_n$ 中定义 $\bar{a}+\bar{b}=\overline{a+b}$,则 $\mathbf{Z}_n$ 也是群.但注意 $\bar{a}+\bar{b}=\overline{a+b}$ 就是



$$(a+n\mathbf{Z})+(b+n\mathbf{Z})=(a+b)+n\mathbf{Z}.$$

我们自然要问，当 H 是 G 的子群时，对于 $aH,bH\in S_L$ 定义

$$(aH)\circ(bH)=(ab)H,$$

那么 S_L 也是群吗？若 $\circ$ 是 S_L 上的二元运算，我们说 S_L 就是群：

(1) 满足结合律：结合律相当于 $((ab)c)H=(a(bc))H$，而由 G 中的结合律知这是明显的；

(2) 有单位元 $eH=H$：

$$(aH)(eH)=(ae)H=aH;$$
$$(eH)(aH)=(ea)H=aH$$

(3) aH 有逆元 $a^{-1}H$：

$$(aH)(a^{-1}H)=(a^{-1}a)H=eH=H;$$
$$(a^{-1}H)(aH)=(a^{-1}a)H=eH=H.$$

回头看，$\circ$ 是 S_L 上的二元运算的条件是什么？要 $\circ$ 是 S_L 上的二元运算，就要下面的推理可行：

$$aH=a_1H,bH=b_1H\Rightarrow(ab)H=(a_1b_1)H$$

这等同于

$$a_1^{-1}a\in H,b_1^{-1}b\in H\Rightarrow(a_1b_1)^{-1}(ab)=b_1^{-1}a_1^{-1}ab\in H.$$

但由 $aH=a_1H,bH=b_1H$，我们只能得到

$$h_1\equiv a_1^{-1}a\in H,h_2\equiv b_1^{-1}b\in H.$$

但我们注意到

$$b_1^{-1}a_1^{-1}ab=[b_1^{-1}(a_1^{-1}a)b_1](b_1^{-1}b)=(b_1^{-1}h_1b_1)h_2,$$

因而只要 $b_1^{-1}h_1b_1\in H$，就有 $(a_1b_1)^{-1}(ab)=b_1^{-1}a_1^{-1}ab\in H$，即 $(ab)H=(a_1b_1)H$.总之，要 $\circ$ 是 S_L 上的二元运算，应要求子群 H 再满足下列条件：

$$g\in G,h\in H\Rightarrow g^{-1}hg\in H.$$

有趣的是这个要求并不过分，即它是保证 $\circ$ 是 S_L 上的二元运算的充分必要条件.事实上，若 $\circ$ 是 S_L 上的二元运算，则

$$\begin{aligned}g\in G,h\in H&\Rightarrow hH=eH,gH=gH\\&\Rightarrow(hg)H=(eg)H=gH\\&\Rightarrow g^{-1}hg\in H.\end{aligned}$$

定义 (1) N 是群 G 的子群.若 N 再满足下列条件我们就称 N 是 G 的**正规子群**，记为 $N\lhd G$：

$$g\in G,n\in N\Rightarrow g^{-1}ng\in N;$$

(2) 当 $N\lhd G$ 时，$G/N=\{aN|a\in G\}$ 在运算

$$(aN)(bN)=(ab)N$$

之下构成的群称 G 的(模 N 的)**商群**.

例如，$n\mathbf{Z}\lhd\mathbf{Z},\mathbf{Z}_n=\mathbf{Z}/n\mathbf{Z}$.

当商群 G/N 为有限群时,它的阶就是$[G:N]$;又当 G 为有限群时,商群 G/N 的阶$|G/N| = |G|/|N|$.

例 1 任何一个群 G 至少有两个**平凡正规子群**,G 和$\{e\}$.G/G 是单元群,$G/\{e\} \cong G$.

例 2 交换群的每个子群都是正规子群.

例 3 若$\sigma: G \to G'$ 为群同态,则 $\ker\sigma \lhd G$.事实上,我们已知 $\ker\sigma \leqslant G$.现在,任取 $a \in G$,$n \in \ker\sigma$,有

$$\sigma(a^{-1}na) = \sigma(a^{-1})\sigma(n)\sigma(a) = \sigma(a^{-1})\sigma(a)$$
$$= \sigma(a^{-1}a) = \sigma(e) = e' \Rightarrow a^{-1}na \in \ker\sigma.$$

例 4 S_3 的子群 $H = \{(1),(12)\}$ 不是 S_3 的正规子群,因为

$$(13)^{-1}(12)(13) = (23) \notin H.$$

正规子群在群论中极为重要,为此我们给出更多的判别方法.

定理 1 设 N 是群 G 的子群,则以下四项是等价的:

(1)$N \lhd G$;

(2)$a^{-1}Na \subset N(a \in G)$;

(3)$a^{-1}Na = N(a \in G)$;

(4)$Na = aN(a \in G)$.

证明 (1)⇒(2) 由正规子群的定义可证;

(2)⇒(3) $aNa^{-1} \subset N(a \in G) \Rightarrow N = eNe = a^{-1}(aNa^{-1})a$

$$\subset a^{-1}Na \subset N \Rightarrow a^{-1}Na = N;$$

(3)⇒(3) 明显成立;

(4)⇒(1) $a \in G, n \in N, Na = aN \Rightarrow na = an'(n' \in N)$

$$\Rightarrow a^{-1}na = n' \in N.$$

例 5 群 G 的**中心** $C(G)$ 是与 G 中每个元都可交换的元的集合,$C(G) \lhd G$.事实上,$C(G)$ 是子群是明显的;又若 $a \in G, z \in C(G)$,则有 $a^{-1}za = (a^{-1}a)z = z \in C(G)$.

例 6 $A_n \lhd S_n$.事实上,我们已知 $A_n \leqslant S_n$,又对任何$\alpha \in S_n$,$\alpha^{-1}A_n\alpha$ 中的置换为偶置换,故 $\alpha^{-1}A_n\alpha \subset A_n$ 成立.特别是,对于 S_3,因为对换(13),(12),(23) 为奇置换,而 $S_n(n \geqslant 2)$ 中奇置换和偶置换各占一半,故

$$A_3 = \{(1),(123),(132)\} \lhd S_3,$$

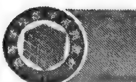
$[S_3 : A_3] = 2$,商群 $S_3/A_3 = \{A_3,(12)A_3\}$.

习题 2 – 6

1.若 $N \lhd G$,且$|N| = 2$,则 G 的中心包含 N.

2.证明,两个正规子群的交也是正规子群.

3.若$[G:N] = 2$,则 $N \lhd G$.



4.若 $H \leqslant G, N \lhd G$ 则 $HN \leqslant G$.

5.群 G 中可以写成 $[a,b] = a^{-1}b^{-1}ab$ 形式的元称**换位子**.证明:

(1) 所有有限个换位子的乘积之集 C 是 G 的正规子群;

(2) G/C 是交换群;

(3) 若商群 G/N 是交换群,则 $C \subset N$.*

2.7 群的同构与正规子群

在正规子群,商群与同态之间存在几个极为重要的关系.从这些重要的关系中我们才可看到正规子群和商群的重要地位.

我们首先有下述定理.

定理 1 若 $N \lhd G$,则 $G \geqslant G/N$,即群与它的每个商群同态.

证明 令 $\pi: a \mapsto aN$,π 明显是满射;又我们有

$$\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b),$$

即 π 是同态.总之,$G \geqslant G/N$.

对于群 G,当我们有一个正规子群 N,我们就又多了两个群,N 和商群 G/N.当然,若 G/N 与原来的群 G 失去了联系,它的意义就不大了,但上述定理告诉我们 G 与 G/N 同态,这样,我们可由 G/N 来推测 G 的性质.

正规子群的重要性还体现在另一个方面.

若 $\sigma: G \mapsto G'$ 是群 G 到群 G' 的满同态.由第一章最后一节的同态基本定理我们知道,对任意 $a, b \in G$,若定义

$$a \sim b \Leftrightarrow \sigma(a) = \sigma(b),$$

则 $\sim$ 是 G 上的等价关系,G 的等价类集合 $G/\sim = \{\bar{a} \mid a \in G\}$ 在运算

$$\bar{a} \circ \bar{b} = \overline{ab}$$

之下与 G' 同构,同构为 $\bar{\sigma}: \bar{a} \mapsto \sigma(a)$.当然此时,$G/\sim$ 也是群了.现在,我们就看一看 $G/\sim$ 中的元 $\bar{a}$ 是什么? 事实上,

$$b \in \bar{a} \Leftrightarrow \sigma(b) = \sigma(a) \Leftrightarrow \sigma(a^{-1}b) = e' \Leftrightarrow a^{-1}b \in \ker\sigma \Leftrightarrow b \in a\ker\sigma,$$

即 $\bar{a} = a\ker\sigma$, $G/\sim = G/\ker\sigma$.总之,我们有下面的重要定理.

定理 2 若 σ 是群 G 到群 G' 的满同态,则 $G/\ker\sigma \cong G'$.

以上两个定理说明,本质上讲,一个群的一切商群包罗了这个群的一切同态像,而商群与正规子群一一对应.再次我们看到了正规子群的重要性.

另外,当 $\sigma: G \mapsto G'$ 是满同态时,$\sigma^{-1}(e') = \ker\sigma \lhd G$.事实上,在这个同态下 G 与 G' 的子群和正规子群间有如下更一般的关系.

定理 3 若 σ 是群 G 到群 G' 的同态,则我们有如下结论:

(1)$H \leqslant G \Rightarrow \sigma(H) \leqslant G'$;

(2)$N \lhd G \Rightarrow \sigma(N) \lhd G'$;

(3)$H' \leqslant G' \Rightarrow \sigma^{-1}(H') \leqslant G$;

(4)$N' \lhd G' \Rightarrow \sigma^{-1}(N') \lhd G$.

证明 我们仅证(1)和(2),其它情况类似.设 $H \leqslant G$.任取 $\sigma(a),\sigma(b) \in \sigma(H) \neq \varnothing$.由 $H \leqslant G$,我们有 $ab^{-1} \in H$,进而,得到

$$\sigma(a)\sigma(b)^{-1} = \sigma(a)\sigma(b^{-1}) = \sigma(ab^{-1}) \in \sigma(H),$$

即 $\sigma(H) \leqslant G'$.再设 $N \lhd G$,由前部分,我们知 $\sigma(N) \leqslant G'$.任取 $\sigma(a) \in G' = \sigma(G)$,$\sigma(n) \in \sigma(N)$.由 $N \lhd G$,我们有 $a^{-1}na \in N$,从而得到

$$\sigma(a)^{-1}\sigma(n)\sigma(a) = \sigma(a^{-1})\sigma(n)\sigma(a) = \sigma(a^{-1}na) \in \sigma(N),$$

即 $\sigma(N) \lhd G'$.

在数学中,在某种运算或变换下,对象的不变性是非常重要的.我们看到子群和正规子群就具有同态运算下的不变性.

习题 2－7

1.证明群的满同态 $\sigma: G \mapsto G'$ 是同构 $\Leftrightarrow \ker\sigma = \{e\}$.

2.直接证明定理 2.

3.若群 G 与群 G' 同态,同态为 σ,$N' \lhd G'$,$N = \sigma^{-1}(N')$.证明 $G/N \cong G'/N'$.

4.若 G 和 G' 是两个有限循环群.证明,G 与 G' 同态 $\Leftrightarrow |G'|$ 整除 $|G|$.

5.若 G 是限循环群,$N \leqslant G$.证明 G/N 也是循环群.

2.8 群在集合上的作用

1 群在集合上的作用

群在计数方面有广泛的应用,这主要源于模型化的 Burnside 定理,此定理涉及群在集合上的作用.事实上,若 G 为集合 X 上的变换群,除了 G 本身作为群有自身的性质外;另一方面,从几何的角度,我们也可以借助 G 来探讨集合 X,而 G 本质上靠下列方式作用在 X 上:

(1)$1_X(x) = x(x \in X)$;

(2)$(hg)(x) = h(g(x)) \quad (g,h \in G;x \in X)$.

抽其本质,我们定义群在集合上的作用.

定义 设 G 为群,X 为集合.若存在 $G \times X$ 到 X 的运算 $*$ 满足下列条件:

(1)$e * x = x(x \in X)$;

(2)$(hg) * x = h * (g * x) \quad (g,h \in G;x \in X)$,



则我们称 G **通过** $*$ **作用在** S **上**.在上下文清楚时,我们简写 $g*x$ 为 gx.

例 1 S_n 自然地作用在集合 $\{1,2,\cdots,n\}$ 上.

例 2 G 为群,$X=G$,则 $g*x=gx$ 定义了一个 G 在自身上的作用——**左平移作用**.

例 3 G 为群,$X=G$,则 $g*x=gxg^{-1}$ 也定义了一个 G 在自身上的作用——**共轭作用**.事实上,$e*x=exe^{-1}=x$,且

$$\begin{aligned}(hg)*x&=(hg)x(hg)^{-1}=(hg)x(g^{-1}h^{-1})\\&=h(gxg^{-1})h^{-1}=h(g*x)h^{-1}\\&=h*(g*x).\end{aligned}$$

定义 设群 G 作用在集合 X 上,$x\in X$:

(1) 我们称 X 的子集

$$Gx\equiv\{gx\mid g\in G\}\subset X$$

为 x 在 G 作用下的**轨道**;

(2) 我们称 G 的子群(易证)

$$\text{stab}x\equiv\{g\in G\mid gx=x\}<G$$

为 x 在 G 中的**稳定化子**.

例 4 设群

$$G=\{(1),(12),(345),(354),(12)(345),(12)(354)\}\leqslant S_5,$$
$$X=\{1,2,3,4,5\}.$$

令 G 自然地作用在 X 上.求 X 所有轨道和 G 的所有稳定化子.

解 直接计算,我们得到两个轨道,两个稳定化子:

$$G1=G2=\{1,2\},$$
$$G3=G4=G5=\{3,4,5\};$$
$$\text{stab}1=\text{stab}2=\{(12),(345),(354)\}\leqslant G,$$
$$\text{stab}3=\text{stab}4=\text{stab}5=\{(1),(12)\}\leqslant G.$$

以下我们讨论轨道和稳定化子的基本性质.

引理 1 设群 G 作用在 X 上,则

$$\Pi\equiv\{Gx\mid x\in X\}\subset p(X)$$

为集合 X 的一个分类.

证明 (1) 对任何 $x\in X$,有 $ex=x\in Gx$,故

$$X=\bigcup_{x\in X}Gx;$$

(2) 令 $Gx\cap Gy\neq\varnothing$,则存在 g_1,g_2 使 $g_1x=g_2y$,从而

$$x=g_1^{-1}(g_2y)=(g_1^{-1}g_2)y\in Gy,$$

进而 $Gx\subset Gy$.对称地,有 $Gy\subset Gx$,从而 $Gx=Gy$.

引理 2 设群 G 作用在 X 上,$x\in X$,$[G:\text{stab}x]$ 有限,则

$$|Gx| = [G:\mathrm{stab}x].$$

（注：对于集合 A，$|A|$ 表示 A 中的元素个数.）

证明 设 $H=\mathrm{stab}x$，$S_L=\{gH|g\in G\}$ 为 H 在 G 中的左陪集的集合，下面的推理证明了 $\sigma: gx\mapsto gH$ 为 Gx 到 G/H 的双射：

$$g_1x=g_2x\Leftrightarrow(g_2^{-1}g_1)x=x\Leftrightarrow g_2^{-1}g_1\in H\Leftrightarrow g_1H=g_2H.$$

由上述两引理我们可得到下面的重要定理.

定理 1 设群 G 作用在 X 上，$x\in X$，X 为有限集，则

$$|X| = \sum\nolimits_{x\in R}[G:\mathrm{stab}x],$$

这里 R 为 X 诸轨道的代表元之集.

评注：通过不同的作用群 G 和被作用集合 X 及不同的作用方式，我们可以得到许多重要的 $|X| = \sum_{x\in R}[G:\mathrm{stab}x]$ 等式.例如，对于 G 在自身上的共轭作用，$Gx=\{x\}\Leftrightarrow x\in C$（$G$ 的中心）.若 G 为有限群，则我们得到一个很重要的等式——**有限群的类方程**：

$$|G| = |C| + \sum\nolimits_{x\in R-C}[G:\mathrm{stab}x].$$

例 5 空间正多面体的一切旋转对称构成一个群——旋转群.求正方体旋转群 G 的阶数.

解 如果我们一个一个地数，则很麻烦且容易遗漏.我们用公式 $|Gx|=[G:\mathrm{stab}x]$ 的变种

$$|G| = |Gx|\cdot|\mathrm{stab}x|$$

就很容易了.任选正方体的一个顶点 x，此点可以对称旋转到原来的任何一个顶点处，即 $|Gx|=8$.同样，保持顶点 x 不变的对称旋转有 3 个（旋转 $0°$，$120°$，$240°$），$|\mathrm{stab}x|=3$.从而有

$$|G| = 8\times 3 = 24.$$

2　Burnside 定理

定理 2(Burnside) 设群 G 作用于 X 上，G 和 X 都有限，则 X 在 G 的作用下不同轨道的个数

$$n = \frac{1}{|G|}\sum\nolimits_{g\in G}|F_g|,$$

这里 $F_g=\{x\in X|gx=x\}\subset X$ 是 g 在 X 上不动点的集合.

证明 令 $X=Gx_1\cup\cdots\cup Gx_n$ 为 X 的不交的轨道分解.

我们将以纵横两个不同的途径讨论 $G\times X$ 的子集

$$T\equiv\{(g,x)\in G\times X|gx=x\}$$

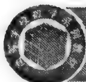
中元素的计数：

(1) 若固定 g，去选合适的 x，则

$$T^g\equiv\{(g,x)|gx=x, x\in X\}$$

与 F_g 一一对应，从而

$$|T| = \sum\nolimits_{g\in G}|T^g| = \sum\nolimits_{g\in G}|F_g|;$$



(2) 若固定 x,去选合适的 g,则

$$T_x \equiv \{(g,x) \mid gx = x, g \in G\}$$

与 stab$x$ 一一对应,从而

$$|T| = \sum_{x\in X}|T_x| = \sum_{x\in X}|\text{stab}x| = \sum_{g\in G}|F_g|.$$

再由引理 1,

$$\sum_{x\in X}|\text{stab}x| = \sum_{x\in X}\frac{|G|}{|Gx|} = |G|\left(\sum_{x\in Gx_1}\frac{1}{|Gx|} + \cdots + \sum_{x\in Gx_n}\frac{1}{|Gx|}\right)$$

再注意到,当 $x,y \in Gz$ 时,$Gx = Gy = Gz$,从而 $\sum_{x\in Gz}\frac{1}{|Gx|}$ 为 $|Gz|$ 个 $\frac{1}{|Gz|}$ 的和,为 1,故 $\sum_{x\in X}|\text{stab}x| = |G|\cdot n$.总之,我们得到

$$n = \frac{1}{|G|}\sum_{x\in X}|\text{stab}x| = \frac{1}{|G|}\sum_{g\in G}|F_g|.$$

例 6 由例 4,我们可以验证上述定理:

$$F_{(1)} = \{1,2,3,4,5\}, F_{(12)} = \{3,4,5\}, F_{(345)} = F_{(354)} = \{1,2\},$$

$$F_{(12)(345)} = F_{(12)(354)} = \varnothing;$$

$$n = \frac{1}{|G|}\sum_{g\in G}|F_g| = \frac{12}{6} = 2.$$

习题 2 - 8

1.设群 G 作用于 X 上,$x \in X$,求证 $\text{stab}\,gx = g(\text{stab}x)g^{-1}$.

2.设 G 为群,$H \leqslant G$,$S_L = \{aH \mid a \in G\}$.对任何 $g \in G$,$aH \in S_L$,定义 $g(aH) = gaH$.证明这定义了一个 G 在 S_L 上的作用,并确定轨道和稳定化子.

3.证明 p^m(p 为素数)阶群 G 的中心 C 不只含有单位元.*

第3章　环　　论

在前一章中，我们讨论了群这个代数结构，群只有一个二元运算.但有时我们常常需要有两个运算的代数结构，而且这两个运算是有机结合的.本章中，我们讨论环和域，它们就有两个运算，其中一个对另一个满足分配律.

3.1　环的基本概念

1　环的定义

定义　(1) 若代数结构$(R,+,\circ)$满足下列条件，称 R 为环：

①$(R,+)$是加群；

②$(R,\circ)$满足结合律：$(ab)c=a(bc)$；

③ 乘法$\circ$对加$+$法满足分配律：

$$a(b+c)=ab+ac,$$
$$(b+c)a=ba+ca;$$

(2) R 是环，称 R 是**有单位元的环**，若 R 中乘法有一个单位元，即存在一个元素 1，对于 R 中任何元素 a，有

$$a1=1a=a.$$

(3) R 是环，且乘法满足交换律，称 R 是**交换环**；

(4) R 是有单位元 1 的环，$a\in R$，称 a **可逆**，若有 $b\in R$ 使

$$ab=ba=1\ (\text{可证明 } b \text{ 唯一，记 } b=a^{-1}).$$

例1　$\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$都是有单位元的交换环，单位元就是1，零元是0；$\mathbf{Z}$在中仅有$1,-1$可逆；在$\mathbf{Q},\mathbf{R},\mathbf{C}$中非零元都可逆.

例2　一切偶数之集$2\mathbf{Z}$对加法和乘法也构成一个交换环，不过此环没有单位元.

例3　$(\mathbf{Z}_n,+,\circ)$是一个有单位元的有限交换环，单位元就是$\overline{1}$，零元是$\overline{0}$:乘法满足结合律是明显的；乘法对于加法满足分配律也是明显的；$\overline{1}$明显为单位元.$\mathbf{Z}_n$的元$\overline{k}$可逆的条件是$(k,n)=1$(见本节习题5).例如，在$\mathbf{Z}_4$中，$\overline{1}$的逆元是自身；$\overline{3}$的逆元也是自身：$\overline{3}\cdot\overline{3}=\overline{3\cdot 3}=\overline{9}=\overline{1}$；$\overline{2}$没有逆元.

注：在环$\mathbf{Z}_n$中，以后我们用0表示$\overline{0}$，用1表示$\overline{1}$.

例4　一切$n\times n(n\geqslant 2)$实矩阵之集$M_n(\mathbf{R})$对矩阵的加法和乘法构成一个有单位元的



非交换环，单位元是单位阵，零元是零矩阵，可逆元就是可逆阵.

环有很多种类，下面的定理给出了它们的一些共同的性质.

定理 1 若 R 为环，则它有下列性质：

(1)$0a = a0 = 0$;

(2)$(-a)b = a(-b) = -(ab)$;

(3)$(-a)(-b) = ab$;

(4)$(na)b = a(nb)(n \in \mathbf{Z})$;

(5)$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$;

(6)单位元若存在，必唯一；

(7)在有单位元的环中，可逆元的逆元也唯一.

证明 我们仅证明(1) 和(2)，其它留作练习.

(1)$0a = (0+0)a = 0a + 0a \Rightarrow 0a = 0$，同理 $a0 = 0$;

(2) $ab + (-a)b = (a + (-a))b = 0b = 0 \Rightarrow (-a)b = -(ab)$,

$ab + a(-b) = a(b + (-b)) = a0 = 0 \Rightarrow a(-b) = -(ab)$.

2 零因子与整环

我们注意到 $\mathbf{Z}$ 与 $\mathbf{Z}_6$ 有一个很大的区别. 在 $\mathbf{Z}$ 中，若 $a \neq 0, b \neq 0$，则必有 $ab \neq 0$；在 $\mathbf{Z}_6$ 中，$\bar{2} \neq 0, \bar{3} \neq 0$，但是 $\bar{2} \cdot \bar{3} = 0$.

定义 在环 R 中，若 $ab = 0$，但 $a \neq 0, b \neq 0$，则我们称 a 是一个**左零因子**，b 是一个**右零因子**. 左零因子和右零因子统称**零因子**.

例如，$\bar{2},\bar{3},\bar{4}$ 是 $\mathbf{Z}_6$ 中的零因子；$\mathbf{Z}$ 中没有零因子；环 $M_2(\mathbf{R})$ 有零因子，例如，$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ 为零因子.

定义 我们称环 R 为**整环**，若它再满足下列条件：

(1)乘法满足交换律：$ab = ba$;

(2)有单位元 1：$a1 = 1a = a$;

(3)至少有两个不同的元：$1 \neq 0$;

(4)没有零因子：$a \neq 0, b \neq 0 \Rightarrow ab \neq 0$.

例如，$\mathbf{Z}$ 是最典型的整环；$\mathbf{Q},\mathbf{R},\mathbf{C}$ 也是整环；$\mathbf{Z}_2$ 是元素最少的整环；$\mathbf{Z}_6$ 不是整环，$\bar{2},\bar{3},\bar{4}$ 是零因子.

例 5 求证，当 p 是一个素数时，$\mathbf{Z}_p$ 是整环.

证明 我们只要证明 $\mathbf{Z}_p$ 没有零因子. 事实上，

$$\bar{m} \neq 0, \bar{n} \neq 0 \Rightarrow p \nmid m, p \nmid n \Rightarrow p \nmid mn \Rightarrow \bar{m}\bar{n} = \overline{mn} \neq 0.$$

3 无零因子环的特征

有零因子的环与无零因子的环的加群有一个极为重要的本质区别,我们对比 $\mathbf{Z},\mathbf{Z}_5$ 和 $\mathbf{Z}_6$:

(1)$\mathbf{Z}$ 中,所有的非零元的阶都相同:无限;

(2)$\mathbf{Z}_5$ 中,所有的非零元的阶都相同:5;

(3)$\mathbf{Z}_6$ 中,$o(\bar{1})=6,o(\bar{2})=3,o(\bar{3})=2,o(\bar{4})=3,o(\bar{5})=6.$

事实上,我们有如下重要的定理.

定理 2 若 R 是无零因子的环,则其加群中所有非零元的阶相同,或是无限,或是一个素数.

证明 设 a,b 是 R 中的两个非零元,n 是任何正整数.由于 R 无零因子,故下列推理成立:

$$na=0\Leftrightarrow(na)b=a(nb)=0\Leftrightarrow nb=0,$$

这就说明 R 中所有非零元的阶相同,或是无限,或是有限数 p.当为有限数 p 时,我们说这个 p 一定为素数.若不然,$p=kl,1<k<p,1<l<p$.此时,对任何非零元 a 有

$$(ka)(la)=(kl)a^2=pa^2=0\Rightarrow ka=0\text{ 或 }la=0,$$

这与 p 是 a 的阶矛盾.

定义 若 R 是无零因子环,当其加群中所有非零元的阶无限时,我们称 R 是**特征 0 的**,记为 $\mathrm{ch}R=0$;当此阶为素数 p 时,我们称 R 是**特征 p 的**,记为 $\mathrm{ch}R=p$.

例如,环 $\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$ 都是特征 0 的;p 是素数时,$\mathrm{ch}\mathbf{Z}_p=p$.

评注:在特征 p 的交换环中,我们有如下有趣的公式:

$$(a\pm b)^p=a^p\pm b^p.$$

这是因为,当 $ab=ba$ 时,

$$(a+b)^p=a^p+C_p^1a^{p-1}b+\cdots+C_p^{p-1}ab^{p-1}+b^p;$$

又因为当 $C_p^1,\cdots,C_p^{p-1}$ 是 p 的倍数时,

$$C_p^1a^{p-1}b=\cdots=C_p^{p-1}ab^{p-1}=0.$$

例 6 在特征为 2 的环中,如 $\mathbf{Z}_2$ 中,有 $a=-a$,这是因为

$$a+a=2a=0.$$

习题 3-1

1. 证明任何一个加群都可作成一个环.

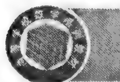
2. 若一个环 R 对于加法是循环群.证明此环是交换环.

3. 证明 $\{m+n\sqrt{2}\mid m,n\in\mathbf{Z}\}$ 对于普通加法和乘法作成一个环.

4. 证明,在有单位元的环中,加法的交换律可由其它条件推出.

5. 证明,$\mathbf{Z}_n$ 的元 $\bar{k}$ 可逆 $\Leftrightarrow(k,n)=1$.

6. 在一个环中,若对于某个正整数 m,有 $a^m=0$,我们说 a 是**幂零元**.证明,在交换环中,两个幂零元的和还是幂零元.找一个有非零幂零元的有限环.



7.证明,在环 R 中,下面两条是等价的:

(1) R 没有非零幂零元;

(2) 若 $a^2 = 0$,则 $a = 0$.

8.在环 R 中,若对于任何元 a,有 $a^2 = a$,我们称此环为**布尔环**.证明布尔环是交换环,且 $2a = 0$.

9.环 R 有 $1, a, b \in R$.证明 $1 - ab$ 可逆 $\Leftrightarrow 1 - ba$ 可逆.*

3.2 除环与域

定义 (1) 我们称环 R 为**除环**,若 R 还满足下列条件:

① 有单位元 1;

② 至少有两个元:$1 \neq 0$;

③ 非零元之集 R^* 对于乘法构成一个群.

(2) 乘法可交换的除环称为**域**.

评注:(1) 除环一定没有零因子,这是因为

$$a \neq 0, ab = 0 \Rightarrow b = a^{-1}(ab) = 0.$$

(2) 在域内,若 $b \neq 0$,有 $b^{-1}a = ab^{-1}$,我们可用 $\frac{a}{b}$ 表示 $b^{-1}a = ab^{-1}$.此时,普通分数的运算法则在域中也成立,如

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

例 1 $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ 都是域,且它们的特征都是 0.

例 2 $\mathbf{Z}_2$ 是元最少的域,特征为 2.

例 3 求证,当 p 是一个素数时,$\mathbf{Z}_p$ 是域.

证明 我们已知 $\mathbf{Z}_p$ 为整环,$1 \neq 0$,$\mathbf{Z}_p^*$ 对于乘法封闭,乘法满足结合律和交换律.现在我们只要证明它的每个非零元都可逆,而下面的推理说明了这一点:

$$\bar{n} \neq 0 \Rightarrow p \nmid n \Rightarrow (p, n) = 1 \Rightarrow ap + bn = 1 \Rightarrow \overline{ap + bn} = \bar{1} \Rightarrow \bar{b}\bar{n} = \bar{1}.$$

以后我们将给出特征为 $p \neq 0$ 的无限域的例子.

存在有限的非域的除环吗?我们的回答是不存在.

定理 1(Wedderburn) 有限除环一定为域.

此定理有初等证明方法,但难度超出了本课程的范围.

至此,我们要问有没有不是域的除环,回答是肯定的.当然,这样的例子不是好找的.至少定理 1 告诉我们在有限集合中是找不到的.下面给出的非交换的 Hamilton 除环(**四元数除环**)在代数史上是很有地位的,它是复数域的推广.

例 4 令 $\mathbf{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$.约定

$$a \equiv a + 0\mathrm{i} + 0\mathrm{j} + 0\mathrm{k}, \quad 0 \equiv 0 + 0\mathrm{i} + 0\mathrm{j} + 0\mathrm{k}, 1 \equiv 1 + 0\mathrm{i} + 0\mathrm{j} + 0\mathrm{k}.$$

我们可在 $\mathbf{H}$ 上如下定义加法和乘法使其成为一个非交换的除环：

$$\begin{aligned} +:&(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}) + (\alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k}) \\ &= (a+\alpha) + (b+\beta)\mathrm{i} + (c+\gamma)\mathrm{j} + (d+\delta)\mathrm{k}; \\ \circ:&(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}) \circ (\alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k}) \\ &= (a\alpha - b\beta - c\gamma - d\delta) + (a\beta + b\alpha + c\delta - d\gamma)\mathrm{i} \\ &\quad + (a\gamma - b\delta + c\alpha + d\beta)\mathrm{j} + (a\delta + b\gamma - c\beta + d\alpha)\mathrm{k}. \end{aligned}$$

上述加法的定义很自然，完全例行公事地可验证 $(\mathbf{H}, +)$ 是加群，0 是零元. 上述的乘法在表面上很玄妙，实际上，只要我们默认分配律，再按下列规则运算即可：

(1) $a\mathrm{i} = \mathrm{i}a, \quad a\mathrm{j} = \mathrm{j}a, \quad a\mathrm{k} = \mathrm{k}a$;

(2) $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$;

(3) $\mathrm{ij} = -\mathrm{ji} = \mathrm{k}, \quad \mathrm{jk} = -\mathrm{kj} = \mathrm{i}, \quad \mathrm{ki} = -\mathrm{ik} = \mathrm{j}$.

同样，完全例行公事地可验证乘法满足结合律，1 是乘法单位元，乘法对加法满足分配律. 现在我们要说明 $\mathbf{H}$ 中每个非零元 $z = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ 都有逆元. 事实上，令 $\bar{z} = a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k}$，当 $z \neq 0$，时

$$\begin{aligned} z\bar{z} &= (a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k})(a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k}) \\ &= a^2 - ab\mathrm{i} - ac\mathrm{j} - ad\mathrm{k} + ba\mathrm{i} - b^2\mathrm{i}^2 - bc\mathrm{ij} - bd\mathrm{ik} \\ &\quad + ca\mathrm{j} - cb\mathrm{ji} - c^2\mathrm{j}^2 - cd\mathrm{jk} + da\mathrm{k} - db\mathrm{ki} - dc\mathrm{kj} - d^2\mathrm{k}^2 \\ &= a^2 + b^2 + c^2 + d^2, \\ z^{-1} &= (a^2 + b^2 + c^2 + d^2)^{-1}\bar{z}; \end{aligned}$$

又 $\mathrm{ij} \neq \mathrm{ji}$，故 $\mathbf{H}$ 是非交换除环.

评注：在第 5 章中，我们将证明，对任何一个素数 p 和任何一个正整数 n，在同构的意义下存在唯一的一个有限域含有 p^n 个元素. 以后我们用 $\mathbf{F}_q$ 表示含有 q 个元素的有限域.

习题 3 - 2

1. 若 F 是有 4 个元的域. 证明

(1) F 的特征是 2;

(2) F 的不是 0 和 1 的两个元都满足方程 $x^2 = x + 1$.

2. 证明 $\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ 对于普通加法和乘法构成一个域.

3. 证明，整环的乘法满足消去律，从而证明有限整环为域.

4. 令 $\bar{a} \in \mathbf{Z}_n$. 证明，若 $(a, n) = 1$，则 $\bar{a}$ 中的任何数都同 n 互素. 此时，我们说 $\bar{a}$ 与 n **互素**.

5. 证明，$\mathbf{Z}_n$ 中与 n 互素的一切元构成一个乘法群. 此群的阶我们用 $\phi(n)$ 表示.

6. 证明，若 $(a, n) = 1$，则 $a^{\phi(n)} \equiv 1 (\bmod n)$. *

3.3 子环和环同态

我们已看到,子群和群同态在群的研究中很重要.在环的研究中我们也完全有与之平行的子环和环同态.它们的作用也完全类似.

1 子环

定义 S是环R的一个子集,若S对R上的加法和乘法也构成环,我们就称S是R的**子环**,记为$S \leqslant R$;同理我们可定义**子整环**,**子除环和子域**.

定理 1 设是环R的子集S.若

$$a,b \in S \Rightarrow a-b,ab \in S$$

则$S \leqslant R$.

例 1 任何一个环R都两个**平凡子环**,R和$\{0\}$.

例 2 偶数环$2\mathbf{Z}$是整数环$\mathbf{Z}$的子环,但前者没有单位元.

例 3 $\mathbf{Z} \leqslant \mathbf{Q} \leqslant \mathbf{R}$, $M_n(\mathbf{Z}) \leqslant M_n(\mathbf{Q}) \leqslant M_n(\mathbf{R})$.

2 环同态与同构

定义 (1)R和R'为环,映射$\sigma:R \to R'$称为R到R'的同态,若σ再满足下列条件:

$$\sigma(a+b)=\sigma(a)+\sigma(b), \quad \sigma(ab)=\sigma(a)\sigma(b);$$

(2) 若$\sigma:R \to R'$为环同态,且为满射,则称σ满同态,同时称R与R'同态,记为$R \geqslant R'$;

(3) 若$\sigma:R \to R'$为环的满同态,且为单射,则称σ为同构,同时称R与R'同构,记为$R \cong R'$;

(4) 若$\sigma:R \to R'$为环同态,$0'$为R'的零元,我们称

$$\ker\sigma \equiv \sigma^{-1}(0')=\{a \in R \mid \sigma(a)=0'\}$$

为σ的核.

例 4 整数环$\mathbf{Z}$与环$\mathbf{Z}_n$同态.很明显$\sigma:a \mapsto \bar{a}$为所需的满同态:

$$\sigma(a+b)=\overline{a+b}=\bar{a}+\bar{b}=\sigma(a)+\sigma(a);$$

$$\sigma(ab)=\overline{ab}=\bar{a}\cdot\bar{b}=\sigma(a)\cdot\sigma(b).$$

例 5 (四元数除环的另一种实现)在$M_2(\mathbf{C})$中,取其四个元:

$$\boldsymbol{E}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\boldsymbol{I}=\begin{bmatrix}\mathrm{i} & 0\\0 & -\mathrm{i}\end{bmatrix},\boldsymbol{J}=\begin{bmatrix}0 & 1\\-1 & 1\end{bmatrix},\boldsymbol{K}=\begin{bmatrix}0 & \mathrm{i}\\\mathrm{i} & 0\end{bmatrix}$$

经过计算,我们得到如下结果:

$$\boldsymbol{I}^2=\boldsymbol{J}^2=\boldsymbol{K}^2=-\boldsymbol{E};$$

$$\boldsymbol{I}\cdot\boldsymbol{J}=-\boldsymbol{J}\cdot\boldsymbol{I}=\boldsymbol{K},\boldsymbol{J}\cdot\boldsymbol{K}=-\boldsymbol{K}\cdot\boldsymbol{J}=\boldsymbol{I},\boldsymbol{K}\cdot\boldsymbol{I}=-\boldsymbol{I}\cdot\boldsymbol{K}=\boldsymbol{J}.$$

令$\mathbf{H}'=\{a\boldsymbol{E}+b\boldsymbol{I}+c\boldsymbol{J}+d\boldsymbol{K} \mid a,b,c,d \in \mathbf{R}\}$,则由上面的算式及 Hamilton 除环$\mathbf{H}$中运算

的定义,我们确信,由 $\mathbf{H}$ 到 $\mathbf{H}'$ 的映射

$$\sigma: a + bi + cj + dk \longmapsto aE + bI + cJ + dK$$

为双射,且保持加法和乘法运算.这就证明了 $\mathbf{H}'$ 为环 $M_2(\mathbf{C})$ 的子环,且与 $\mathbf{H}$ 同构.

定理 2 设 $\sigma: R \to R'$ 为环同态,则

(1)$\sigma(0)$ 是 R' 的零元;

(2)$\sigma(-a) = -\sigma(a)$;

(3)$\ker\sigma \leqslant R$;

(4)σ 为单同态 $\Leftrightarrow \ker\sigma = \{0\}$.

此定理的证明较简单,留给读者练习.

定理 3 若 σ 是环 R 到环 R' 的满同态,则我们有下列结论:

(1) 若 1 是 R 的单位元,则 $\sigma(1)$ 是 R' 的单位元;

(2) 若 $S \leqslant R$,则 $\sigma(S) \leqslant R'$;

(3) 若 $S' \leqslant R'$,则 $\sigma^{-1}(S') \leqslant R$.

注:本定理中,仅有(1) 需要 σ 为满同态.

评注:无零因子性质不是同态不变性.例如,$\sigma: a \longmapsto \bar{a}$ 是环 $\mathbf{Z}$ 到环 $\mathbf{Z}_4$ 的满同态,但前者无零因子,而后者有零因子 $\bar{2}$.

3 环的嵌补

时常我们要从已知的环来造新的环,如由整数环造有理数域,下面的嵌补定理是我们的理论基础.

定理 4(嵌补定理) 若环 S' 同构于环 R 的一个子环 S,则存在一个与 R 同构的环 R' 使得 S' 在保持原有的运算时,是 R' 的子环.

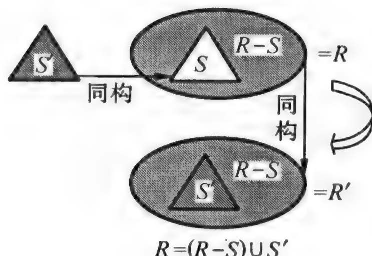


图 3-1

证明 下面的图 3-1 直观地说明由 R 造 R' 的过程:

令 φ 是 $S' = \{a', b', \cdots\}$ 到 $S = \{a, b, \cdots\}$ 的同构, $x' \leftrightarrow x$; $R = \{x, y, \cdots \mid a, b, \cdots\}$ 中的加法和乘法分别为 $+, *$.造集合

$$R' \equiv \{x, y, \cdots \mid a', b', \cdots\} = (R - S) \cup S'.$$

现在我们定义一个由 R' 到 R 的一一对应 σ 如下:

$$x \leftrightarrow x, y \leftrightarrow y, \cdots \quad (x, y, \cdots \in R - S);$$

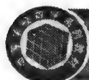
$$a' \leftrightarrow a, b' \leftrightarrow b, \cdots \quad (a', b', \cdots \in S');$$

σ 限制在 S' 上与 φ 一致.

如下定义 R' 上的加法 $\oplus$ 和乘法 $\otimes$:

$$\alpha \oplus \beta = \sigma^{-1}(\sigma(\alpha) + \sigma(\beta));$$

$$\alpha \otimes \beta = \sigma^{-1}(\sigma(\alpha) * \sigma(\beta));$$



例行公事,我们可验证$(R',\oplus,\otimes)$是环,σ是R'到R的同构;又由于σ限制在S'上与φ一致,故R'上的运算限制到S'上与S'上原来的运算一样,故S'是R'的子环.

评注:此定理说明我们完全可以将S中的元与S'中相应的元等同.事实上,我们已经这样做了.例如,复数域含有一个子域$\{a+0\mathrm{i}\mid a\in\mathbf{R}\}$与实数域同构,因而就将实数$a$与复数$a+0\mathrm{i}$等同了,也将实数域视为复数域的一个子域了.

我们可以这样不严格地来理解这个定理.假设有本小说R,其中有一章S除了人物和地点名称外,故事情节完全与另一本小说S'雷同.我们若将R中的S章节用S'替换造出新书R'(此时,R'是不和谐的),保持S'完全不变(包括人物和地点的名称),而参照S与S'的对应更改R中其它章节中的人物和地点名称.这时,新书R'就是一本完全和谐的小说,与原来的R完全雷同且S'(保持不变)为其一部分.

习题 3-3

1. R是环,我们称$Z(R)\equiv\{a\in R\mid ar=ra(r\in R)\}$为$R$的**中心**.证明一个环的中心是一个交换子环(本身为交换环的子环).
2. 证明一个除环的中心是域.
3. 证明特征为0的域都含有一个与有理数域同构的子域.
4. 找出加群$\mathbf{Z}_3$的一切自同构和域$\mathbf{Z}_3$的一切自同构.
5. 证明域$\mathbf{Q}(\mathrm{i})=\{a+\mathrm{i}b\in\mathbf{C}\mid a,b\in\mathbf{Q}\}$仅有两个自同构.*

3.4 多项式环

多项式在许多学科中有重要的应用.其实,关于多项式的一些概念我们还不是非常清楚的.例如,我们早就被定义式地告知,若$a+bx+cx^2=\alpha+\beta x+\gamma x^2$,则$a=\alpha,b=\beta,c=\gamma$.可是$a+bx+cx^2$是什么呢?$x$与$a,b,c$的地位一样吗?若一样,当$1+3\cdot2+(-4)\cdot2^2=(-9)+0\cdot2+0\cdot2^2$时,为什么$1\neq-9,3\neq0,-4\neq0$?当然我们会说$x$与普通的数不一样,可不同在何处?下面我们将给出一个明确的说明.在本节中我们一直假设R_0和R是有单位元1的交换环,且R是环R_0的子环.

1 一元多项式

定义 若R,R_0如前所述,$\alpha\in R_0$,我们称R_0中的元

$$a_0+a_1\alpha+\cdots+a_n\alpha^n\quad(n\in\mathbf{N},a_i\in R)$$

为α在R上的一个**多项式**,称a_i为此多项式的**系数**.

定理1 R上的α的一切多项式构成R_0的一个子环,1是它的单位元.我们用$R[\alpha]$表示此环,称其为R上的α的**多项式环**.

例如,取 $R_0 = \mathbf{R}$ 为实数域,则$\sqrt{2}$在有理数域 $\mathbf{Q}$ 上的多项式环为

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\},$$

这是因为 $a + b\sqrt{2}$ 是$\sqrt{2}$在 $\mathbf{Q}$ 上的多项式,而$(\sqrt{2})^n$ $(n \in \mathbf{N})$ 是整数或整数与$\sqrt{2}$的乘积.事实上,$\mathbf{Q}[\sqrt{2}]$ 是域.但$\sqrt{2}$在 $\mathbf{Q}$ 上的多项式与我们熟知 $\mathbf{Q}$ 的上的 x 多项式有所不同.例如,

$$1 + 1 \cdot \sqrt{2} + 1 \cdot (\sqrt{2})^2 = 3 + 1 \cdot \sqrt{2} + 0 \cdot (\sqrt{2})^2,$$

即$\sqrt{2}$在 $\mathbf{Q}$ 上的多项式的系数不唯一.但系数唯一的多项式是很重要的.

定义 (1)R_0 中的元 x 称为 R 上的一个未定元,若

$$a_0 + a_1 x + \cdots + a_n x^n = 0 (n \in \mathbf{N}, a_i \in R)$$
$$\Rightarrow a_0 = \cdots = a_n = 0;$$

(2) 若 x 为 R 上的一个未定元,当 $a_n \neq 0$ 时,我们称

$$a_0 + a_1 x + \cdots + a_n x^n$$

为 x 的一个 n 次多项式.

定理 2 给定一个有单位元的交换环 R,一定存在一个环含有 R 上的一个未定元 x,因此存在 R 上未定元 x 的多项式环 $R[x]$.

证明 首先我们用环 R 构造一个环 P':

(1) 令

$$P' = \{(a_0, a_1, \cdots) \mid a_0, a_1, \cdots \in R \text{ 中仅有有限个不是 } 0\};$$

(2)P' 的加法:

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots),$$

很明显$(P', +)$是加群,零元 $0 = (0, 0, \cdots)$;

(3)P' 的乘法:

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \cdots).$$

例行公事,我们可验证 P' 对上述运算封闭,满足结合律,交换律,$(1, 0, 0, \cdots)$ 是单位元;此乘法对于前面的加法满足分配律.总之,P' 对上述定义的加法和乘法构成一个有单位元的交换环.

(4)P' 中含有一个与 R 同构的子环

$$R' = \{(a, 0, \cdots) \mid a \in R\}, (a, 0, \cdots) \leftrightarrow a;$$

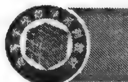
(5) 由上一节的嵌补定理,用 R 替换 P' 中的 R',我们可得到一个与 P' 同构的环 P,P 的单位元就是 R 的单位元 1.

(6)P 含有 R 上的未定元 x:

$$x = (0, 1, 0, \cdots).$$

首先,由 P 中乘法的定义,我们很容易验证:

$$x^k = (0, \cdots, 0, 1, 0, \cdots) \quad (1 \text{ 的前面有 } k \text{ 个 } 0);$$



若在 P 中，

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

则在 P' 中

$$(a_0,0,\cdots) + (a_1,0,\cdots)x + \cdots + (a_n,0,\cdots)x^n = (0,0,\cdots),$$
$$(a_0,a_1,\cdots,a_n,0,\cdots) = (0,0,\cdots),$$

从而 $a_0 = a_1 = \cdots = a_n = 0$.这说明 x 是 R 上的未定元.

例 1 现在我们给出一个特征为素数 p 的无限域:任取一个特征为 p 的域 F,如 $\mathbf{Z}_p$,x 为 F 上的未定元.令

$$F(x) = \left\{\frac{f(x)}{g(x)}\middle| f(x),g(x) \in F[x] \quad (g(x) \neq 0)\right\}$$

则对普通有理式的加法和乘法,$F(x)$ 是特征为 p 的无限域.$1,x,\cdots,x^n,\cdots$ 是 $F(x)$ 中的无限个不同的元.

2 未定元的泛性

定理 3 若 $R[x]$,$R[\alpha]$ 都是有单位元交换环 R 上的多项式环,且 x 为 R 上的无关未定元,则

$$\sigma: f(x) \mapsto f(\alpha)$$

是 $R[x]$ 到 $R[\alpha]$ 的满同态.

为什么说上面的定理重要,因为它道出了未定元的一个重要的本质:未定元的可替换性或未定元的泛性.事实上,从上面 $R[x]$ 和 $R[\alpha]$ 的构造过程我们应注意到:$R[x]$ 中的未定元 x 与 $R[\alpha]$ 中的 α 完全可以来自两上不同的环.但若在 $R[x]$ 中有关系式 $f(x) + g(x) = h(x)$,$f(x)g(x) = k(x)$,则由定理 4,我们有 $R[\alpha]$ 中的关系式

$$f(\alpha) + g(\alpha) = h(\alpha), \quad f(\alpha)g(\alpha) = k(\alpha)$$

但注意,α 与 R 只要能容纳在同一个环中,此环与 R 有相同的单位元,都可交换.

习题 3 - 4

1.证明,若 R 是整环,则 $R[x]$ 也是整环.

2.在 $\mathbf{Z}_7[x]$ 中,计算$(3x^3 + 5x - 4)(4x^2 - x + 3)$.

3.p 为素数.证明 $\mathbf{Z}_p[x]$ 中的多项式 $x^{p^2} - x^p + 1$ 可约,即能分解成两个次数更小的多项之积.

3.5 理想与商环

1 理想

在群论中,我们已经看到正规子群和商群在群的研究中是非常重要的.在环论中,我们也

有完全平行的理论，与正规子群对应的是环的理想，与商群对应的是商环.为此我们先考察环 $\mathbf{Z}_n$ 的构造过程.

首先，$n\mathbf{Z} = \{na \mid a \in \mathbf{Z}\}$ 是整数环 $\mathbf{Z}$ 的加群的一个正规子群，$\mathbf{Z}_n$ 就是商群 $\mathbf{Z}/n\mathbf{Z}$，在 $\mathbf{Z}_n$ 中定义

$$(a + n\mathbf{Z})(b + n\mathbf{Z}) = (ab) + n\mathbf{Z},$$

$\mathbf{Z}_n$ 就作成了一个环.

现在我们提出这样一个问题：假设 I 是环 R 的加群的一个子群，我们就有一个加群 $R/I = \{a + I \mid a \in I\}$.此时，若我们在 R/I 上定义

$$(a + I)(b + I) = (ab) + I,$$

那么 R/I 能作成一个环吗？

事实上，若上面定义是合理的，即是一个运算，则按环的定义，例行公事，我们可验证 R/I 是一个环.那么我们要问，在什么条件下上面的定义是合理的，即下列推理成立：

$$a + I = a_1 + I, \quad b + I = b_1 + I \Rightarrow ab + I = a_1 b_1 + I,$$

这等同于

$$a - a_1, \quad b - b_1 \in I \Rightarrow ab - a_1 b_1 \in I;$$

但我们只有下面的推理

$$\begin{aligned} a - a_1, \quad b - b_1 \in I &\Rightarrow a = a_1 + i_1, b = b_1 + i_2 (i, i_2 \in I) \\ &\Rightarrow ab = a_1 b_1 + a_1 i_2 + i_1 b_1 + i_1 i_2 \\ &\Rightarrow ab - a_1 b_1 = a_1 i_2 + i_1 b_1 + i_1 i_2. \end{aligned}$$

若要求 I 是子环，我们有 $i_1 i_2 \in I$，但我们还无法保证 $a_1 i_1$，$i_1 b_1 \in I$ 都成立.但我们看到若 I 再满足下列条件(I 已经是加群 R 的子群了)，就有 $i_1 i_2 \in I$ 和 $a_1 i_2, i_1 b_1 \in I$，从而 $ab - a_1 b_1 \in I$，即上述定义的就是 R/I 上的运算了：

$$r \in R, \ i \in I \Rightarrow ri, \ ir \in I.$$

有趣的是这个要求并不过分，即它是保证上述定义的是 R/I 上二元运算的充分必要条件.事实上，若定义合理，则

$$\begin{aligned} r \in R, \ i \in I &\Rightarrow r + I = r + I, \quad i + I = 0 + I \\ &\Rightarrow ri + I = r0 + I = I, \quad ir + I = 0r + I = I \\ &\Rightarrow ir, \quad ir \in I. \end{aligned}$$

定义 (1) I 是环 R 的子环，若 I 再满足下列条件我们就称 I 是 R 的**理想**，记为 $I \lhd R$：

$$r \in R, \ i \in I \Rightarrow ri, \ ir \in I;$$

(2) 当 $I \lhd R$ 时，加群 $R/I = \{a + I \mid a \in R\}$ 在乘法

$$(a + I)(b + I) = (ab) + I$$

之下构成的环称 R 的(模 I 的) **商环**.

例如，$n\mathbf{Z} \lhd \mathbf{Z}, \mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$.



例 1 每个环 R 都有两个平凡理想,**零理想** $\{0\}$ 和**单位理想** R 本身.$R/\{0\}\cong R, R/R\cong\{0\}$.

例 2 若 $\sigma: R\to R'$ 为环同态,则 $\ker\sigma\lhd R$.事实上,我们已知 $\ker\sigma$ 为 R 的子环;另一方面,我们有

$$r\in R,\ a\in\ker\sigma\Rightarrow\sigma(ra)=\sigma(r)\sigma(a)=0,$$
$$\sigma(ar)=\sigma(a)\sigma(r)=0$$
$$\Rightarrow ra,\ ar\in\ker\sigma.$$

例 3 除环只有平凡理想.事实上,假设 I 是除环 D 的一个非零理想,$a\in I, a\neq 0$,则 $aa^{-1}=1\in I$,进而

$$d\in D, 1\in I\Rightarrow d=d1\in I\Rightarrow D\subset I\Rightarrow D=I.$$

上面的例子说明理想对于除环和域没有什么意义.

例 4 若 R 是有单位元的交换环,则 $R[x]$ 中常数项为 0 的一切多项式之集 (x) 是 $R[x]$ 的理想,且 $R[x]/(x)\cong R$.事实上,(x) 是 $R[x]$ 的理想是明显的;另一方面,若

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$

则 $f(x)+(x)=a_0+(x)$,因而

$$\sigma: f(x)+(x)\mapsto a_0$$

就是 $R[x]/(x)$ 到 R 的同构.若 F 是域,此例说明 $F[x]/(x)$ 就是域.

2 生成理想

给了一个环 R,我们常常在 R 中取一些元:$a_1,\cdots,a_n$ 探讨 R 中包含 $a_1,\cdots,a_n$ 的最小理想是什么样的?我们称这个理想为 $a_1,\cdots,a_n$ 生成的**生成理想**,记为 $(a_1,\cdots,a_n)$.为了看看 $(a_1,\cdots,a_n)$ 是什么样,我们先取一个 $a\in R$.由于 $a\in(a)$,再由理想的定义我们知

$$x,y,s,t\in R, n\in\mathbf{Z}\Rightarrow xay, sa, at, na\in(a)$$
$$\Rightarrow\sum xay+sa+at+na\in(a);$$

反之,一切 $\sum xay+sa+at+na$ 的集合恰好是 R 的含 a 的理想.因为两个这样元的差还是这样的;R 中任何一个元无论从左边还是右边乘这样的元,结果还是这样的.

定义 我们称理想

$$(a)=\left\{\sum xay+sa+at+na\,|\,x,y,s,t\in R, n\in\mathbf{Z}\right\}$$

为由 a 生成的**主理想**.

评注:(1) 当 R 是交换环时,$xay=xya, at=ta$,从而

$$(a)=\{ra+na\,|\,r\in R, n\in\mathbf{Z}\};$$

(2) 当 R 有单位元时,$sa=sa1, at=1at, na=(n1)a1$,从而

$$(a)=\left\{\sum xay\,|\,x,y\in R\right\};$$

(3) 当 R 有单位元,又可交换时,

$$(a) = \{ra \mid r \in R\};$$

(4) $(a_1,\cdots,a_n) = \{s_1 + \cdots + s_n \mid s_i \in (a_i)\}$.

事实上,例4中的理想就是 $R[x]$ 的主理想 (x).不过,并不是每个理想都是主理想,见本节习题7.

3 环的同态定理

与群的同态定理完全平行,我们有环的同态定理.

定理1 若 $I \lhd R$,则 R 与 R/I 同态.

证明 令 $\pi: r \longmapsto r + I$.例行公事,我们可验证 π 是 R 到 R/I 的满同态.

定理2 若 σ 是环 R 到 R' 的满同态,则 $R/\ker\sigma \cong R'$.

证明 令 $\bar{\sigma}: r + \ker\sigma \longmapsto \sigma(r)$,容易验证,此映射是 $R/\ker\sigma$ 到 R' 的同构.

最后我们指出,理想是同态不变性.

定理3 若 σ 是环 R 到 R' 的同态,则我们有

(1) $I \lhd R \Rightarrow \sigma(I) \lhd R'$;

(2) $I' \lhd R' \Rightarrow \sigma^{-1}(I') \lhd R$.

证明 此定理的证明与群中一样,留作练习.

习题 3-5

1. 若 $R = 2\mathbf{Z}$ 是偶数环,证明 $I = \{4r \mid r \in R\}$ 是 R 的理想. $I = (4)$ 成立吗?
2. 证明,在 $\mathbf{Z}$ 中, $\{3,7\}$ 生成的理想 $(3,7) = (1)$.
3. 证明,在 $\mathbf{Q}[x]$ 中, $\{2,x\}$ 生成的理想 $(2,x)$ 是主理想.
4. 证明两个理想的交还是理想.
5. 找出环 $\mathbf{Z}_6$ 的所有理想.
6. 假定环 $R = \{a + bi \mid a, b, \in \mathbf{Z}\}$,那么环 $R/(1 + i)$ 有多少个元素?
7. 证明,在 $\mathbf{Z}[x]$ 中, $\{2,x\}$ 生成的理想 $(2,x)$ 不是主理想.*

3.6 极大理想 商域

以上几节是关于环的一般理论的.以下我们讨论如何由一个交换环来造一个域.例如,由整数环 $\mathbf{Z}$,我们至少可以造两个域, $\mathbf{Z}/(p) = \mathbf{Z}_p$ (p 为素数) 和 $\mathbf{Q}$.本节我们就推广这两种方法.

1 极大理想

定义 一个环 R 的理想 M 称为 R 的一个**极大理想**,假若 $M \neq R$,且在 M 和 R 之间不再



有其它理想，即

$$M \subset I \lhd R, M \neq I \Rightarrow I = R.$$

例 1 若 p 是素数，则 (p) 是整数环 $\mathbf{Z}$ 的极大理想. 事实上，若 $(p) \subset I \lhd \mathbf{Z}, I \neq (p)$，则有 $q \in I, q \notin (p) = p\mathbf{Z}$，即 $p \nmid q$，从而 $(p, q) = 1$. 于是，存在 $s, t \in \mathbf{Z}$ 使 $sp + tq = 1 \in I$. 这说明 $I = \mathbf{Z}$.

例 2 我们已知，当 F 是域时，$F[x]/(x) \cong F$ 是域. 我们说 (x) 是 $F[x]$ 的极大理想. 若 $(x) \subset I \lhd F[x], I \neq (x)$，则 I 一定有一个元 $f(x) \notin (x) = \{xg(x) \mid g(x) \in F[x]\}$，$f(x)$ 的常数项 $a_0 \neq 0$. 于是，

$$f(x) = xh(x) + a_0 \Rightarrow a_0 = f(x) - xh(x) \in I$$

$$\Rightarrow 1 = a_0 a_0^{-1} \in I \Rightarrow I = F[x].$$

事实上，我们有更一般的结论.

定理 1 设 R 是一个有单位元的交换环，M 是 R 的理想，则 M 是 R 的极大理想 $\Leftrightarrow R/M$ 为域.

证明 $(\Rightarrow)$ 设 M 是 R 的极大理想. 由于 $M \neq R$，故 R/M 中的单位元 $1 + M$ 与零元 $0 + M$ 不同；令 $a + M \neq M$，则 $a \notin M$. 造 R 的由 $\{a\} \cup M$ 生成的理想 (a, M)，我们容易证明

$$(a, M) = \{s + m \mid s \in (a), m \in M\}.$$

由于 $M \subset (a, M), a \notin M$，故 $(a, M) = R$. 于是，

$$\begin{aligned} 1 = ra + m \in (a, M) &\Rightarrow ra - 1 \in M \\ &\Rightarrow ra + M = 1 + M \\ &\Rightarrow (r + M)(a + M) = 1 + M, \end{aligned}$$

即 $a + M$ 在 R/M 中可逆. 从而 R/M 为域.

$(\Leftarrow)$ 设 R/M 为域. 由于 $1 + M \neq 0 + M$，故 $M \neq R$. 现在假设 $I \lhd R$，且 $M \subset I, M \neq I$. 令 $a \in I, a \notin M$. 由于 $a + M \neq 0 + M$，R/M 是域，故存在 $b + M$ 使

$$(a + M)(b + M) = ab + M = 1 + M,$$

即 $ab - 1 = i \in M \subset I$. 于是，$1 = ab - i \in I \Rightarrow I = R$，这说明 M 是 R 的极大理想.

2 商域

现在我们讨论通过扩大一个环来构造域的方法. 例如，整数环就可以扩大成有理数域. 由于域没有零因子，且可交换，因而能扩大成域的环是无零因子的交换环. 我们说此条件足够了.

定理 2 每个无零因子的交换环 R 都是一个域的子环.

证明 以下我们由 R 构造一个含 R 的域，本质上，其过程与整数造有理数的过程一样.

$R^* \equiv R - \{0\}$，我们在 $R \times R^* = \{(a, b) \mid a \in R, b \in R^*\}$ 上定义一个关系：

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc;$$

完全例行公事，我们可验证 $\sim$ 是 $R \times R^*$ 上的一个等价关系. 我们用 $\frac{a}{b}$ 表示 (a, b) 所在的等价

类,记等价类的集合为

$$Q = \left\{\frac{a}{b} \mid a \in R, b \in R^*\right\}.$$

在 Q 上我们定义加法和乘法如下:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b}\,\frac{c}{d} = \frac{ac}{bd};$$

同样,完全例行公事,我们可验证 Q 对上面的加法和乘法构成一个域,且

$$0 = \frac{0}{b}, \quad 1 = \frac{b}{b}, \quad -\frac{a}{b} = \frac{-a}{b} \quad (a \neq 0);$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \quad (a, b \neq 0).$$

若我们定义 $\sigma: a \longmapsto \frac{ab}{b}$,则 σ 是 R 到 Q 的子环

$$R' = \left\{\frac{ab}{b} \mid a \in R\right\}$$

的同构.我们用 a 替换 Q 中的$\frac{ab}{b}$.此时,

$$ab^{-1} = b^{-1}a = \frac{ab}{b}\,\frac{c}{cb} = \frac{a}{b},$$

而且

$$Q = \{ab^{-1} \mid a \in R, b \in R^*\}.$$

定义 设 R 为无零因子的交换环.若域

$$Q = \{ab^{-1} \mid a \in R, b \in R^*\},$$

则我们称 Q 是 R 的**商域**.

评注:(1) 每个无零因子的交换环 R 都有商域;

(2) 由上面的构造我们看到同构的环,其商域也必然同构;

(3) 不同构的环,其商域可以同构.例如,整数环 $\mathbf{Z}$ 和偶数环 $2\mathbf{Z}$ 的商域都是有理数域 $\mathbf{Q}$.

(4) 包含环 R 的任何域 F 都包含 R 的一个商域.事实上,若域 F 包含环 R,令 $Q = \{ab^{-1} \mid a \in R, b \in R^*\}$,则 Q 是 R 的商域.

习题 3-6

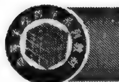
1.若环 $R = \{a + b\mathrm{i} \mid a, b \in \mathbf{Z}\}$,证明 $R/(1 + \mathrm{i})$ 是域.

2.(x) 是不是 $\mathbf{Z}[x]$ 的极大理想?(x) 是不是 $\mathbf{Q}[x]$ 的极大理想?

3.若交换环 R 有非零的单位元,只有平凡理想.证明此环是域.

4.证明,(4) 是偶数环 $2\mathbf{Z}$ 的极大理想,但 $2\mathbf{Z}/(4)$ 不是域.*

5.设 R 为整环,$a, b \in R, a^m = b^m, a^n = b^n$,这里 m, n 为两个互素的正整数.求证 $a = b$.*



6. 求证多项式 x^2+x+1 在 $\mathbf{Z}_2[x]$ 内不可约(不能分解为次数更小的两个多项式的乘积),且主理想 $I=(x^2+x+1)$ 为 $\mathbf{Z}_2[x]$ 的极大理想;$\mathbf{Z}_2[x]/I$ 为 4 个元素的域.列出此域的元素,并写出此域的乘法表和加法表.

第4章　域上多项式的因式分解

整环上，特别是域上多项式环在许多方面有其重要的应用.在这一章中我们将讨论域上多项式环的一个重要性质——唯一分解性，此性质也是域上多项式环的应用基础.在本章的最后一节，我们将指出数域上的多项式环的分解特性.无特别声明，本章中 $F[x]$ 表示域 F 上的未定元 x 的多项式环，$\partial(f)$ 表示多项式 $f(x)$ 的次数.

4.1　多项式的整除

1　多项式的整除

我们知道，整数环 **Z** 有唯一分解性，即任何一个非零整数 a 都可唯一地分解为 $a=\pm p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$，这里 $p_1,p_2,\cdots,p_t$ 是素数.在本章中，我们将证明多项式环 $F[x]$ 也有类似的性质.首先我们在环中要定义'整除'和'不可约多项式'，不可约多项式相当于整数环 **Z** 中的素数.

定义　设 $f(x),g(x)\in F[x]$，若存在 $h(x)\in F[x]$ 满足

$$f(x)=g(x)h(x),$$

则我们称 $g(x)$ **整除** $f(x)$，记为 $g(x)\mid f(x)$，并称 $g(x)$ 为 $f(x)$ 的**因式**，或称 $f(x)$ 是 $g(x)$ 的**倍式**；若 $g(x)$ 不是 $f(x)$ 的因式，记为 $g(x)\nmid f(x)$.

我们知道，讨论整数的整除时，最基本的方法是带余除法，在讨论多项式的整除性时我们同样可用**带余除法**.

例1　在 $\mathbf{Q}[x]$ 内我们有下面**多项式的长除法**：

$$\begin{array}{r|l} & 3x+13 \\ \hline x^2-3x+1 & 3x^3+4x^2-5x+6 \\ & \underline{3x^3-9x^2+3x\quad} \\ & \quad 13x^2-8x+6 \\ & \quad \underline{13x^2-39x+13} \\ & \quad\quad 31x-7 \end{array}$$

上式相当于下面的分解式：

$$3x^3+4x^2-5x+6=(3x+13)(x^2-3x+1)+(31x-7).$$



例 2 在 $\mathbf{Z}_3[x]$ 内我们有下面多项式的长除法：

$$
\begin{array}{r|l}
 & \quad\quad\quad x^2+2 \\
\cline{2-2}
x-1 & x^3+2x^2+2x+1 \\
 & x^3-x^2 \\
\cline{2-2}
 & \quad\quad\quad 2x+1 \\
 & \quad\quad\quad 2x-2 \\
\cline{2-2}
 & \quad\quad\quad\quad\quad 0
\end{array}
$$

上式相当于下面的分解式：

$$x^3+2x^2+2x+1=(x-1)(x^2+2).$$

定理 1(带余除法) 若 $f(x),g(x)\in F[x],g(x)\neq 0$,则存在唯一的 $q(x),r(x)\in F[x]$ 使

$$f(x)=q(x)g(x)+r(x),$$

其中 $\partial(r)<\partial(g)$ 或 $r(x)=0$.这里,称 $q(x)$ 为 $g(x)$ 除 $f(x)$ 的商式;$r(x)$ 为 $g(x)$ 除 $f(x)$ 的余式.

证明 (存在性)

(1)$f(x)=0$:此时,取 $q(x)=r(x)=0$.

(2) 设 $f(x)\neq 0,\partial(f)=n,\partial(g)=m$.

①$n<m$:此时,取 $q(x)=0,r(x)=f(x)$;

②$n\geqslant m$:此时,用例 1 所示的多项式长除法,我们可得到满足条件的 $q(x),r(x)$.

(唯一性) 设 $q_1(x),r_1(x)$ 也使

$$f(x)=q_1(x)g(x)+r_1(x),$$

其中 $\partial(r_1)<\partial(g_1)$ 或 $r_1(x)=0$.于是,

$$q(x)g(x)+r(x)=q_1(x)g(x)+r_1(x),$$

从而

$$(q(x)-q_1(x))g(x)=r_1(x)-r(x).$$

若 $q(x)-q_1(x)\neq 0$,又因 $g(x)\neq 0$,则

$$r_1(x)-r(x)\neq 0,\partial(q-q_1)+\partial(g)=\partial(r_1-r);$$

另一方面,$\partial(r_1-r)<\partial(g)$,因而 $\partial(q-q_1)+\partial(g)=\partial(r_1-r)$ 不能成立,从而

$$q(x)-q_1(x)=0,\quad r(x)-r_1(x)=0,$$

即满足条件的 $q(x),r(x)$ 唯一.

推论 若 $f(x),g(x)\in F[x]$, $g(x)\neq 0$,则 $g(x)\mid f(x)\Leftrightarrow g(x)$ 除 $f(x)$ 的余式 $r(x)=0$.

2　最大公因式

公因式:若 $h(x)\mid f(x)$,$h(x)\mid g(x)$,则称 $h(x)$ 为 $f(x)$ 和 $g(x)$ 的**公因式**.

最大公因式:若 $d(x)$ 为 $f(x)$ 和 $g(x)$ 公因式,且 $d(x)$ 能被 $f(x)$ 和 $g(x)$ 任何一个公因式整除,则称 $d(x)$ 为 $f(x)$ 和 $g(x)$ 的**最大公因式**.

评注:(1) 若 $d_1(x),d_2(x)$ 都为 $f(x),g(x)$ 的最大公因式,则 $d_1(x)\mid d_2(x)$,$d_2(x)\mid d_1(x)$,从而 $d_1(x)=cd_2(x)\ (c\neq 0)$;若 $f(x),g(x)$ 不全为 0,则它们的最大公因式不是 0,此时我们用 $(f(x),g(x))$ 表示首项系数为 1 的最大公因式.

(2) 若 $f(x)=q(x)g(x)+r(x)$,则 $f(x),g(x)$ 和 $g(x),r(x)$ 有相同的最大公因式.

定理 2　对于任何 $f(x),g(x)\in F[x]$,它们在 $F[x]$ 内存在最大公因式 $d(x)$,而且存在 $u(x),v(x)\in F[x]$ 使

$$d(x)=u(x)\cdot f(x)+v(x)\cdot g(x).$$

证明　(1) 若 $f(x),g(x)$ 中有一个为 0,如 $g(x)=0$,结论成立,且

$$f(x)=1\cdot f(x)+1\cdot g(x)$$

(2) 设 $f(x)g(x)\neq 0$.我们做如下的**辗转相除**,余式为 0 时,停止.为了清晰,假设 $r_3(x)\neq 0$,$r_4(x)=0$:

$$\begin{aligned}
f(x)&=q_1(x)g(x)+r_1(x),\\
g(x)&=q_2(x)r_1(x)+r_2(x),\\
r_1(x)&=q_3(x)r_2(x)+r_3(x),\\
r_2(x)&=q_4(x)r_3(x)+r_4(x)\quad (r_4(x)=0).
\end{aligned}$$

由上述各式我们看出 $r_3(x)$ 为 $r_3(x),r_2(x)$ 的最大公因式;$r_3(x)$ 为 $r_2(x),r_1(x)$ 的最大公因式;$r_3(x)$ 为 $r_1(x),g(x)$ 的最大公因式;$r_3(x)$ 为 $g(x),f(x)$ 的最大公因式:

$$\begin{aligned}
r_3(x)&=r_1(x)-q_3(x)r_2(x)=r_1(x)-q_3(x)[g(x)-q_2(x)r_1(x)]\\
&=r_1(x)k(x)+l(x)g(x)\\
&=[f(x)-q_1(x)g(x)]k(x)+l(x)g(x)\\
&=u(x)f(x)+v(x)g(x).
\end{aligned}$$

例 3　在 $\mathbf{Q}[x]$ 内,令

$$f(x)=x^4+x^3+x^2+2x+1,\quad g(x)=x^3+x^2,$$

求 $(f(x),g(x))$,并求 $u(x),v(x)$ 使

$$(f(x),g(x))=u(x)\cdot f(x)+v(x)\cdot g(x).$$

解　辗转相除如下:



$q_2(x)=x-1$	$g(x)=$ x^3+x^2 x^3+2x^2+x	$f(x)=$ $x^4+x^3+x^2+2x+1$ x^4+x^3	$q_1(x)=x$
	$-x^2-x$ $-x^2-2x-1$	$r_1(x)=x^2+2x+1$ x^2+x	
		$x+1$ $x+1$	$q_3(x)=x+1$,
	$r_2(x)=x+1$	$r_3(x)=0$	

由此我们得到

$$(f(x),g(x))=r_2(x)=x+1;$$

而且

$$x+1=(-q_2)f+(1+q_1q_2)g=(-x-1)f(x)+(x^2-x+1)g(x).$$

3　互素多项式

定义　若$(f(x),g(x))=1$,则我们称$f(x)$和$g(x)$互素.

定理 3　$f(x),g(x)$互素$\Leftrightarrow$存在$u(x),v(x)$使

$$u(x)f(x)+v(x)g(x)=1.$$

证明　由定理2,这是明显的.

定理 4　若$f(x),g(x)$互素,且$f(x)\mid g(x)h(x)$,则

$$f(x)\mid h(x).$$

证明　由定理3,存在$u(x),v(x)$使

$$u(x)f(x)+v(x)g(x)=1,$$

从而

$$u(x)f(x)h(x)+v(x)g(x)h(x)=h(x).$$

于是,$f(x)\mid h(x)$.

评注:最大公因式和互素的概念可以扩展到多个多项式上,而且也有类似的结论.

习题 4－1

1.分别在$\mathbf{Q}[x]$和$\mathbf{Z}_5[x]$中,求$g(x)$除$f(x)$的商式$q(x)$和余式$r(x)$:

(1)$f(x)=x^3-3x^2-x-1,\quad g(x)=3x^2-2x+1$;

(2)$f(x)=x^4-2x+4,\quad g(x)=x^2-x+2$.

2.分别在$\mathbf{Q}[x]$和$\mathbf{Z}_5[x]$中,求$(f(x),g(x))$:

(1)$f(x)=x^4+3x^3-3x^2-4x-1,g(x)=x^3+x^2-x-1$;

(2)$f(x)=x^4-4x^3+1,\quad g(x)=x^3-3x^2+1$.

3.若 $f_1(x)\mid g(x)$,$f_2(x)\mid g(x)$,且$(f_1(x),f_2(x))=1$,求证

$$f_1(x)f_2(x)\mid g(x).$$

4.2　多项式的因式分解

1　不可约多项式

在本节中,我们讨论 $F[x]$ 中多项式的分解问题.在中学,我们学过多项式的因式分解,最终将一个多项式分解到不可再分为止.但我们是靠直观判断不可再分的.事实上,可不可再分是相对的,如在 $\mathbf{Q}[x]$ 内

$$x^4-4=(x^2-2)(x^2+2)$$

不能再分了;但在 $\mathbf{R}[x]$ 内

$$x^4-4=(x-\sqrt{2})(x+\sqrt{2})(x^2+2);$$

又在 $\mathbf{C}[x]$ 内

$$x^4-4=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}\mathrm{i})(x+\sqrt{2}\mathrm{i}).$$

对于不可再分多项式,我们给出严格定义, 即不可约多项式.

定义　多项式 $p(x)\in F[x]$ 称为 F 上的**不可约多项式**,若它的次数 $\geqslant 1$,且在 $F[x]$ 内不能分解成两个次数更小的多项式的乘积;否则称其**可约**.

例　(1) 对于任何域 F,$x+a$ 在 $F[x]$ 内不可约;

(2) x^2-2 在 $\mathbf{Q}[x]$ 内不可约;

(3) x^2+x+1 在 $\mathbf{R}[x]$ 内不可约;

(4) x^3+x^2+x+1 在 $\mathbf{R}[x]$ 内可约,因为

$$x^3+x^2+x+1=(x^2+1)(x+1);$$

(5) x^2+1 在 $\mathbf{Z}_2[x]$ 内可约, 因为 $x^2+1=(x+1)(x+1)$.

不可约多项式的两个基本特性如下:

(1) $p(x)\in F[x]$ 不可约 $\Leftrightarrow$ 它在 $F[x]$ 内的因式仅有非零常数和 $c\cdot p(x)(c\in F,c\neq 0)$;

(2) 若 $p(x)$ 不可约,$f(x)\in F[x]$,则 $p(x)\mid f(x)$ 或 $(p(x),f(x))=1$. 事实上, 若 $(p(x),f(x))=d(x)$,则 $d(x)=1$ 或 $d(x)=c\cdot p(x)(c\neq 0)$,后者为 $p(x)\mid f(x)$.

定理 1　若 $p(x)$ 不可约,且 $p(x)\mid f(x)g(x)$,则 $p(x)\mid f(x)$ 或 $p(x)\mid g(x)$.

证明　设 $p(x)\nmid f(x)$, 则 $(p(x),f(x))=1$.又 $p(x)\mid f(x)g(x)$, 从而 $p(x)\mid g(x)$.

定理 2　域 F 上的任何一个次数 $\geqslant 1$ 的多项式 $f(x)$ 都可分解成 $F[x]$ 中若干不可约多项式的乘积,且若不记因式的次序, 分解是唯一的,即若

$$f(x)=p_1(x)\cdots p_s(x)=q_1(x)\cdots q_t(x)$$



是 $f(x)$ 的两个这样的分解，则 $s=t$，且重排因式的次序后，有

$$p_i(x)=c_iq_i(x), c_i\in P \quad (i=1,\cdots,s).$$

证明 （存在性）若 $f(x)$ 本身不可约，结论成立；否则 $f(x)=f_1(x)f_2(x)$. 此时，若 $f_1(x),f_2(x)$ 都不可约，结论成立. 如此下去，$f(x)$ 可分解成若干不可约多项式的乘积.

（唯一性）设

$$f(x)=p_1(x)\cdots p_s(x)=q_1(x)\cdots q_t(x),$$

$p_1(x),\cdots,p_s(x),q_1(x),\cdots,q_t(x)$ 都不可约，则

$$p_1(x)\mid q_1(x)\cdots q_t(x).$$

由定理 1，$p_1(x)$ 整除 $q_1(x),\cdots,q_t(x)$ 之一. 不妨设 $p_1(x)\mid q_1(x)$. 由于 $p_1(x),q_1(x)$ 都不可约，从而

$$p_1(x)=c_1q_1(x)(c_1\in P,c_1\neq 0).$$

在 $p_1(x)\cdots p_s(x)=q_1(x)\cdots q_t(x)$ 中消去 $p_1(x),q_1(x)$，我们得到

$$p_2(x)\cdots p_s(x)=c_1^{-1}q_2(x)\cdots q_t(x);$$

如此下去，我们可知唯一性成立.

评注：由上述定理，域 F 上的任何一个次数 $\geqslant 1$ 的多项式 $f(x)$ 在 $F[x]$ 都可分解为

$$f(x)=cp_1^{k_1}(x)p_2^{k_2}(x)\cdots p_s^{k_s}(x),$$

这里，c 是 $f(x)$ 的首项系数，$p_1(x),\cdots,p_s(x)$ 为首项系数为 1 的不可约多项式. 上述分解称为 $f(x)$ 的**标准分解式**.

习题 4 - 2

1. 在 $\mathbf{Z}_2[x]$ 内，将 x^3+x^2+x+1 分解成不可约多项式的乘积.
2. 在 $\mathbf{Z}_3[x]$ 内，将 x^3-1 分解成不可约多项式的乘积.
3. 求证，在 $\mathbf{Z}_2[x]$ 内，多项式 $x^4+x^3+x^2+x+1$ 不可约.

4.3 多项式的根

定义 令 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$. 若 $\alpha\in F$ 使

$$f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0,$$

则我们称 α 为 $f(x)$ 在 F 内的**根**

定理 1 α 为 $f(x)$ 在 F 内的根 $\Leftrightarrow (x-\alpha)\mid f(x)$.

证明 由多项式的带余除法，

$$f(x)=q(x)(x-\alpha)+r, \quad r\in F.$$

若 $f(\alpha)=0$，则得到 $r=0$，从而 $(x-\alpha)\mid f(x)$；反之，明显.

推理 1 域 F 中 k 个不同的元 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 为 $f(x)$ 的根 $\Leftrightarrow (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)\mid f(x)$.

推理 2 $F[x]$ 中 $n(n\geqslant 1)$ 次多项式在域 F 内最多有 n 个根.

这两个推理的证明留作习题.

定义 若 $\alpha\in F,(x-\alpha)^k\mid f(x),k>1$,则我们称 α 是 $f(x)$ 的**重根**.

下面,我们讨论判别重根的方法,这需要引入多项式的导数.

多项式的导数:若 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$,则称

$$f'(x)\equiv na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1$$

为 $f(x)$ 的导数.

无疑,多项式的导数来自微积分,它与微分学中导数的运算性质相同.

定理 2 α 是 $f(x)$ 的重根 $\Leftrightarrow x-\alpha$ 为 $f'(x)$ 的因式.

证明 若 α 是 $f(x)$ 的重根,则

$$f(x)=(x-\alpha)^kg(x),k>1,(x-\alpha)\nmid g(x),$$

从而

$$f'(x)=(x-\alpha)^{k-1}[kg(x)+(x-\alpha)g'(x)],$$

这说明 $(x-\alpha)\mid f'(x)$.

若 α 不是 $f(x)$ 的重根,则

$$f(x)=(x-\alpha)g(x),(x-\alpha)\nmid g(x),$$

从而

$$f'(x)=g(x)+(x-\alpha)g'(x),f'(\alpha)=g(\alpha)\neq 0,$$

这说明 $(x-\alpha)\nmid f'(x)$.

由此定理我们得到下面的推理.

推理 若在 $F[x]$ 内 $(f(x),f'(x))=1$,则在域 F 内 $f(x)$ 没有重根.

习题 4 – 3

1. 在 $\mathbf{Q}[x]$ 内,举出一个多项式 $f(x)$,它在 $\mathbf{Q}$ 内没有重根,但

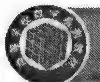
$$(f(x),f'(x))\neq 1.$$

2. 若在 $F[x]$ 内 $(f(x),f'(x))=1$,且 $E\supset F$ 为一个包含 F 的域,求证,在域 E 内 $f(x)$ 仍然没有重根.

3. 求 x^5-x 在 $\mathbf{Z}_5[x]$ 内的标准分解式.

4. 证明定理 1 的推理 1.

5. 证明定理 1 的推理 2.



4.4 数域上的多项式

1 复数域和实数域

代数学基本定理 每个次数 $\geqslant 1$ 的复系数多项式在复数域内至少有一个根.

此定理证明的难度远远超出了本课程的要求,在复变函数论中可以给出较简单的证明.此定理之所以称为代数学基本定理是因为在历史上,代数学曾以一元方程的解为中心,此问题已了结.现代代数学有许多崭新的领域,本定理称为代数学基本定理已成为历史,作为本定理的等价结论,我们有如下重要的定理.

复系数多项式因式分解定理 每个次数 $\geqslant 1$ 的复系数多项式在复数域内都可分解成一次式的乘积,即若 $\mathbf{C}[x]$ 中次数 $\geqslant 1$ 的多项式 $f(x)$ 有如下标准分解式

$$f(x) = a(x-\alpha_1)^{l_1}(x-\alpha_2)^{l_2}\cdots(x-\alpha_s)^{l_s},$$

这里 $\alpha_1,\alpha_2,\cdots,\alpha_s$ 互不相同,$l_1,l_2,\cdots,l_s > 0$.

评注:若 $z\in\mathbf{C}$ 是实系数多项式 $f(x)$ 的根,则 $\bar{z}$ 也是 $f(x)$ 的根,因而 $f(x)$ 的虚部不为0的根共轭成对出现.另一方面,若 $z = a + b\mathrm{i}\ (b\neq 0)$,则

$$(x-z)(x-\bar{z}) = x^2-(z+\bar{z})x+z\bar{z} = x^2-2ax+(a^2+b^2)$$

没有实根.由此我们得到下面的实系数多项式因式分解定理.

实系数多项式因式分解定理 每个次数 $\geqslant 1$ 的实系数多项式在实数域内都可分解成若干一次式和若干二次式的乘积,且这些二次式在实数域内无解.

例如,

$$\begin{aligned}x^5-x^4+x-1 &= (x-1)(x^4+1)\\ &= (x-1)\left[x-\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}\mathrm{i}\right)\right]\left[x-\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}\mathrm{i}\right)\right]\\ &\quad\left[x-\left(-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}\mathrm{i}\right)\right]\left[x-\left(-\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}\mathrm{i}\right)\right]\\ &= (x-1)(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1).\end{aligned}$$

2 有理数域

在有理数域中多项式的分解是复杂的,没有复数域和实数域那样好的结果.我们仅指出两点:

(1) 有理系数多项式的分解可以归结为整系数多项式的分解;

(2) 在有理数域内存在任意次的不可约多项式.

为了导出这两个结论,我们引进本原多项式的概念.

本原多项式:一个非零的整系数多项式称为**本原多项式**,若它的全部系数互素,即它们的

最大公因子为 1.

例如,$3x^5-4x^4+5x-6$ 为本原多项式.

评注:若 $f(x)\in \mathbf{Q}[x]^*$,则 $f(x)$ 可改写为 $f(x)=\frac{a}{b}g(x)$,$g(x)$ 为整系数本原多项式.例如,

$$\frac{2}{3}x^4-2x^2-\frac{2}{5}x=\frac{2}{15}(5x^4-15x^2-3x).$$

定理 1(Gauss) 两个本原多项式的乘积还是本原多项式.

证明 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$
$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$$

为两个本原多项式.假设

$$f(x)g(x)=d_{2n}x^{2n}+d_{2n-1}x^{2n-1}+\cdots+d_1x+d_0$$

不是本原多项式,则存在一个素数 p 能整除 $d_{2n},\cdots,d_1,d_0$.由于 $f(x),g(x)$ 都是本原多项式,因而我们可假设

$$p\mid a_0,\cdots,p\mid a_{i-1},p\nmid a_i;$$
$$p\mid b_0,\cdots,p\mid b_{j-1},p\nmid b_j.$$

我们来看 d_{i+j},由乘积的算法,

$$d_{i+j}=a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_{i-1}b_{j+1}+a_ib_j+a_{i+1}b_{j-1}+\cdots+a_{i+j-1}b_1+a_{i+j}b_0.$$

由于 p 整除 d_{i+j},及上式加项中除了 a_ib_j 以外的每一项,这是矛盾的.

定理 2 若 $f(x)\in \mathbf{Z}[x]$ 在 $\mathbf{Q}[x]$ 内可约,则它在 $\mathbf{Z}[x]$ 内也可约.

证明 设

$$f(x)=g(x)h(x);g(x),h(x)\in \mathbf{Q}[x];\partial(g),\partial(h)<\partial(f),$$

则

$$f(x)=a\cdot f_1(x),\quad g(x)=r\cdot g_1(x),$$
$$h(x)=s\cdot h_1(x),a\in \mathbf{Z},r,s\in \mathbf{Q},$$

这里 $f_1(x),g_1(x),h_1(x)$ 为本原多项式.于是,

$$af_1(x)=(rs)g_1(x)h_1(x);$$

而本原多项式的乘积还是本原多项式,从而 $rs=\pm a$.因此,我们有 $f(x)$ 在 $\mathbf{Z}[x]$ 内的分解式

$$f(x)=[rsg_1(x)]h_1(x).$$

定理 3 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in \mathbf{Z}[x]$,且 r 为 $f(x)$ 的有理根,则 r 为整数,且 $r\mid a_0$.

证明 令 $r=\frac{b}{a}$,$(a,b)=1$.由条件,在 $\mathbf{Q}[x]$ 内,



$$f(x)=q(x)(x-\frac{b}{a})=q_1(x)(ax-b).$$

由于 $f(x),ax-b$ 为本原多项式，很明显 $q_1(x)\in\mathbf{Z}[x]$.于是，

$$f(x)=(b_{n-1}x^{n-1}+\cdots+b_1x+b_0)(ax-b)\quad(b_i\in\mathbf{Z}).$$

比较两边的系数，我们得到 $a=\pm1,b\mid a_0$，从而 $r\mid a_0$.

例1 多项式 x^3-5x+1 在 $\mathbf{Q}[x]$ 内不可约.事实上，若它可约，它必有一个有理根，但它的有理根只可能为 ±1，而 ±1 不是根.

定理4(Eisenstein) 设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbf{Z}[x]$，$p$ 为素数，且

(1) $p\nmid a_n$;

(2) $p\mid a_{n-1},a_{n-2},\cdots,a_0$;

(3) $p^2\nmid a_0$,

则 $f(x)$ 在 $\mathbf{Q}[x]$ 内不可约.

证明 假设 $f(x)$ 在 $\mathbf{Q}[x]$ 内可约，则由定理2，在 $\mathbf{Z}[x]$ 内

$$f(x)=(b_lx^l+\cdots+b_1x+b_0)(c_mx^m+\cdots+c_1x+c_0)(l,m\leqslant n),$$

从而 $a_n=b_lc_m,a_0=b_0c_0$.再由 $p\mid a_0,p^2\nmid a_0\Rightarrow p\mid b_0,p\mid c_0$ 当中仅一个成立，不妨设 $p\mid b_0$，$p\nmid c_0$.

另一方面，$p\nmid a_n=b_lc_m\Rightarrow p\nmid b_l$.设 $b_0,b_1,\cdots,b_l$ 中第一个不能被 p 整除的是 $b_k,k\leqslant l<n$ 现在，比较 $f(x)$ 的 x^k 的系数，得到

$$a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k.$$

由上式，我们得到 $p\mid b_kc_0$，但 $p\nmid b_k,p\nmid c_0$，这是矛盾.

例2 取 $p=2$，由上述定理，x^n+2 在 $\mathbf{Q}[x]$ 内不可约.

习题 4－4

1.求下列整系数多项式的有理根：

(1) $x^3-6x^2+15x-14$;

(2) $x^5+x^4-6x^3-14x^2-11x-3$.

2.当 p 为素数时，割圆多项式

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

求证 $\Phi_p(x+1)$ 在 $\mathbf{Q}[x]$ 内不可约，从而证明 $\Phi_p(x)$ 在 $\mathbf{Q}[x]$ 内不可约.

第5章　域　　论

在这一章中,我们将对域做进一步的讨论,主要内容为单扩域、代数扩域、多项式的分裂域和伽罗瓦域.

5.1　扩　　域

定义　若域 F 是域 E 的子域,我们称 E 为 F 的**扩域**,记为 E/F(从上下文中与商群和商环相区别).

例1　$\mathbf{C}/\mathbf{R}$,$\mathbf{R}/\mathbf{Q}$,$\mathbf{Q}[\sqrt{2}]/\mathbf{Q}$,为扩域.

实数域是在它的子域有理数域上建立起来的,而复数域是在它的子域实数域上建立起来的.研究域的方法就是:从一个给定的域出发来研究它的扩域.

定理1　E 为域.若 E 的特征为0,则它含有一个与有理数域同构的子域.若 E 的特征为素数 p,则它含有一个与 $\mathbf{Z}_p$ 同构的子域.

证明　令 $1\in E$,$\mathbf{Z}'=\{n1\mid n\in\mathbf{Z}\}$,

$$\sigma:\mathbf{Z}\to\mathbf{Z}',n\mapsto n1,$$

σ 明显是整数环 $\mathbf{Z}$ 到 $\mathbf{Z}'$ 的满同态.

(1)$\mathrm{ch}E=0$.这时,σ 为同构:$\mathbf{Z}\cong\mathbf{Z}'$.从而它们的商域也同构,$\mathbf{Z}$ 的商域为有理数域,$\mathbf{Z}'$ 的商域包含在 E 中.

(2)$\mathrm{ch}E=p$.这时,$\ker\sigma=(p)$,$\mathbf{Z}_p=\mathbf{Z}/(p)\cong\mathbf{Z}'$.

素域:一个域所包含的最小子域称为它的**素域**.

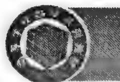
若 E/F 为扩域,$(E,+)$ 为加群;对于任意 $\alpha,\beta\in E$;$k,l\in F$,有 $k\alpha\in E$,$k(\alpha+\beta)=k\alpha+k\beta$,$(k+l)\alpha=k\alpha+l\alpha$,$(kl)\alpha=k(l\alpha)$,$1\alpha=\alpha$,因而 E 可视为 F 上的向量空间.

定义　E/F 为**扩域**.若 E 为 F 上的有限维向量空间,则我们称 E/F 为(F 上)**有限扩域**,此时,我们用$[E:F]$表示 E 在 F 上的**维数**,并称 E 是 F 上的$[E:F]$**次扩域**;否则称其为**无限扩域**.

例2　$\mathbf{R}/\mathbf{Q}$ 为无限扩域;$\mathbf{C}/\mathbf{R}$ 为二次扩域,1,i 是 $\mathbf{C}$ 在 $\mathbf{R}$ 上的基;$\mathbf{Q}[\sqrt{2}]/\mathbf{Q}$ 也为二次扩域,1,$\sqrt{2}$ 是 $\mathbf{Q}[\sqrt{2}]$ 在 $\mathbf{Q}$ 上的基.

定理2　若 E/K,K/F 都是有限扩域($F\subset K\subset E$),则 E/F 也是有限扩域,且

$$[E:F]=[E:K]\cdot[K:F].$$



证明 令 $e_1,e_2,\cdots,e_m$ 为 E 在 K 上的基，$k_1,k_2,\cdots,k_m$ 为 K 在 F 上的基，则 $e_ik_j(i=1,\cdots,m;j=1,\cdots,n)$ 为 E 在 F 上的基. 事实上，

$$\sum_{i,j}f_{ij}(e_ik_j)=0\Rightarrow\sum_i(\sum_j f_{ij}k_j)e_i=0,\sum_j f_{ij}k_j\in K$$
$$\Rightarrow\sum_j f_{ij}k_j=0\Rightarrow f_{ij}=0,$$

这说明 $e_ik_j(i=1,\cdots,m;j=1,\cdots,n)$ 在 F 上线性无关；另一方面，E 中任何一个元都是 e_ik_j $(i=1,\cdots,m;j=1,\cdots,n)$ 在 F 上的线性组合是明显的. 总之，

$$[E:F]=m\cdot n=[E:K]\cdot[K:F].$$

对于扩域 E/F，为了搞清 F 是如何扩张成 E 的，我们可以选择 E 的一个子集 S，特别是 $S=\{\alpha\}$，看一看 E 中包含 F 和 S 的最小子域 $F(S)$ 是什么样的. 我们称 $F(S)$ 为 S 在 F 上的添加.

定理 3 若 E/F 为扩域，$S\subset E$，则 $F(S)$ 由 E 中如下形式的元构成：

$$\frac{f(s_1,\cdots,s_n)}{g(s_1,\cdots,s_n)}$$

这里，n 走遍一切自然数，$f(s_1,\cdots,s_n),g(s_1,\cdots,s_n)\neq 0$ 是 $s_1,\cdots,s_n\in S$ 的多项式.

证明 一方面，E 的任何一个包含 F 和 S 的子域都包含一切上述形式的元；另一方面，E 中一切上述形式的元构成一个含 F 和 S 的子域，因而，E 中一切上述形式的元是含 F 和 S 的最小子域.

定理 4 若 E/F 为扩域，$S_1,S_2\subset E$，则

$$F(S_1)(S_2)=F(S_1\cup S_2)=F(S_2)(S_1).$$

证明 我们仅证 $F(S_1)(S_2)=F(S_1\cup S_2)$.

由于 $F,S_1,S_2\subset F(S_1)(S_2)$，$F(S_1\cup S_2)$ 是包含 F,S_1,S_2 的最小子域，故 $F(S_1)(S_2)\supset F(S_1\cup S_2)$；另一方面，$F(S_1\cup S_2)$ 包含 F,S_1,S_2，因而包含 $F(S_1),S_2$，但 $F(S_1)(S_2)$ 是包含 $F(S_1),S_2$ 的最小子域，从而 $F(S_1)(S_2)\subset F(S_1\cup S_2)$. 于是，

$$F(S_1)(S_2)=F(S_1\cup S_2).$$

定义 扩域 $F(\alpha)/F$ 称为 F 的**单扩域**.

例 3 $\mathbf{Q}(\sqrt{2},\mathrm{i})/\mathbf{Q}$ 为 4 次扩域. 事实上，$\mathbf{Q}(\sqrt{2})(\mathrm{i})/\mathbf{Q}(\sqrt{2})$ 是二次扩域，$\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ 也是二次扩域，而由上述定理 $\mathbf{Q}(\sqrt{2},\mathrm{i})=\mathbf{Q}(\sqrt{2}(\mathrm{i})$. 于是，

$$[\mathbf{Q}(\sqrt{2},\mathrm{i}):\mathbf{Q}]=[\mathbf{Q}(\sqrt{2},\mathrm{i}):\mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2\times 2=4.$$

习题 5－1

1. 证明：(1) $[E:F]=1\Leftrightarrow E=F$；(2) 若 $[E:F]$ 为素数，则 F 和 E 之间没有中间域.
2. 求 $[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}]$ 及 $\mathbf{Q}(\sqrt{2},\sqrt{3})$ 在 $\mathbf{Q}$ 上的一个基.
3. 证明，作为 $\mathbf{Q}$ 上的线性空间，$\mathbf{Q}(\sqrt{2})$ 与 $\mathbf{Q}(\mathrm{i})$ 同构，但作为域它们不同构.

5.2 单扩域

1 单扩域的结构

定义 E/F 为扩域，$\alpha \in E$，若 α 是系数在 F 内的某多项式 $f(x) \in F[x]$ 的根，则我们称 α 为 F 上的**代数元**，此时称 $F(\alpha)/F$ 为**单代数扩域**；否则称 α 为 F 上的**超越元**，此时称 $F(\alpha)/F$ 为**单超越扩域**.

例 1 C/R, $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ 是单代数扩域，而 $\mathbf{Q}(\pi)/\mathbf{Q}$ 是单超越扩域.

定义 若 α 是 F 上的代数元，则 $F[x]$ 中以 α 为根，次数最小的首 1 多项式称 α 在 F 上的**极小多项式**. 它是 $F[x]$ 上的不可约多项式.

例 2 $\sqrt{2}$ 在 $\mathbf{Q}$ 上的极小多项式是 $x^2 - 2$.

定理 1 (1) 若 α 为 F 上的超越元，则

$$F(\alpha) \cong F(x), \quad \alpha \leftrightarrow x,$$

这里 $F(x)$ 是未定元 x 的有理式构成的域，即 $F[x]$ 的商域;

(2) 若 α 为 F 上的代数元，且 α 在 F 上的极小多项式 $p(x)$ 为 n 次的，则

① $F(\alpha) = F[\alpha]$;

② $F(\alpha)$ 中每个元可唯一地表示成

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} (a_0, a_1, \cdots, a_{n-1} \in F);$$

③ $[F(\alpha) : F] = n$.

证明 (1) 当 α 为 F 上的超越元时，

$$\sigma : f(x) \mapsto f(\alpha)$$

明显是 $F[x]$ 到 $F[\alpha]$ 的同构，从而它们的商域也同构. 由本章 5.1 的定理 3, $F(\alpha)$ 为 $F[\alpha]$ 的商域，故

$$F(\alpha) \cong F(x).$$

(2) 当 α 为 F 上的代数元时，

$$\sigma : f(x) \mapsto f(\alpha),$$

是 $F[x]$ 到 $F[\alpha]$ 的满同态，

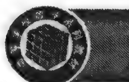
$$F[x]/\ker\sigma \cong F[\alpha].$$

我们断言 $\ker\sigma = (p(x))$.

首先，明显有 $(p(x)) \subset \ker\sigma$.

令 $f(x) \in \ker\sigma$. 由带余除法，

$$f(x) = q(x)p(x) + r(x),$$



这里 $r(x)=0$ 或 $\partial(r)<\partial(p)$.但是,

$$r(\alpha)=f(\alpha)-q(\alpha)p(\alpha)=0$$

说明只有 $r(x)=0$, 进而 $f(x)\in(p(x))$,$\ker\sigma\subset(p(x))$.

$F[x]/(p(x))$ 是域说明 $F[\alpha]$ 是域,而 $F[\alpha]\subset F(\alpha)$,且 F,α 包含在 $F[\alpha]$ 中,故 $F(\alpha)=F[\alpha]$.

另一方面,对任何 $f(x)\in F[x]$,我们有

$$f(x)=q(x)p(x)+r(x),$$

这里 $r(x)=0$ 或 $r(x)$ 的次数小于 $p(x)$ 的次数,从而

$$f(\alpha)=r(\alpha)=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1};$$

再由 $p(x)$ 的极小性,上述 $f(\alpha)$ 的表示是唯一的,即 $1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上线性无关,$[F(\alpha):F]=n$.

例 3 若 p 为素数,$\varepsilon=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$ 在 $\mathbf{Q}$ 上的极小多项为 $x^{p-1}+x^{p-2}+\cdots+x+1$(见习题 4-4-2),故

$$[\mathbf{Q}(\varepsilon):\mathbf{Q}]=p-1.$$

2 单扩域的存在性

到此为止,我们都是在假设扩域 E/F 存在时,来谈论 E 的某些元添加到 F 上的性质.但扩域 E/F 是如何产生的,我们还没有探讨.扩张一个域的方式很多,下面我们仅给出单代数扩张的方式.

定理 1 说明,当 x 为域 F 上的未定元时,$F[x]$ 的商域 $F(x)$ 为 F 的单超越扩域,而且 F 的任何两个单超越扩域都同构.

下面的定理回答了单代数扩域的存在性.

定理 2 若 $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in F[x]$ 是域 F 上的不可约多项式,则存在单代数扩域 $F(\alpha)/F$,其中 α 在 F 上的极小多项式为 $p(x)$;而且任何两个这样的单扩域都同构.

证明 由于 $p(x)$ 在 $F[x]$ 内不可约,故 $I=(p(x))$ 为整环 $F[x]$ 的极大理想.从而,商环 $E=F[x]/I$ 为域.此域含有一个与 F 同构的子域

$$\bar{F}=\{a+I\mid a\in F\},$$

同构为 $\sigma:a\mapsto a+I$.由嵌补定理,我们可将 E 的元 $a+I$ 与 F 的元 a 等同,则 E/F 为扩域.我们说,若令 $\alpha=x+I$,则

$$E=F(\alpha),$$

且 α 在 F 上的极小多项式为 $p(x)$.

首先,E 包含 F 和 α,从而 $F(\alpha)\subset E$;另一方面,对任意 $f(x)=b_0+b_1x+\cdots+b_nx^n\in F[x]$,$E=F[x]/I$ 中的一般元

$$f(x)+I=(b_0+b_1x+\cdots+b_nx^n)+I$$

$$= (b_0 + I) + (b_1 + I)(x + I) + \cdots + (b_n + I)(x + I)^n$$
$$= b_0 + b_1\alpha + \cdots + b_n\alpha^n = f(\alpha) \in F(\alpha),$$

即 $E = F[x]/I \subset F(\alpha)$.总之,$E = F(\alpha)$.又由于 $p(x)$ 在 $F[x]$ 内不可约,且由于 $p(x) \in I$,我们有

$$p(\alpha) = p(x) + I = 0 \in E,$$

故 $p(x)$ 为 α 在 F 上的极小多项式.

由定理 1, 看 $F(\alpha)/F$ 的结构,我们知道任何两个这样的单扩域都同构.

习题 5 – 2

1.i 和$\dfrac{2\mathrm{i}+1}{\mathrm{i}-1}$在 Q 上的极小多项式各是什么?Q(i) 与 Q$(\dfrac{2\mathrm{i}+1}{\mathrm{i}-1})$ 是否同构?

2.令 $E = \mathbf{Q}(u), u^3 - u^2 + u + 2 = 0$.将$(u^2 + u + 1)(u^2 - u)$ 和$(u - 1)^{-1}$ 表示成 $au^2 + bu + c(a,b,c \in \mathbf{Q})$ 的形式.

3.令 $\omega = \cos\dfrac{\pi}{6} + \mathrm{i}\sin\dfrac{\pi}{6}$.证明,$[\mathbf{Q}(\omega):\mathbf{Q}] = 4$,并求 ω 在 Q 上的极小多项式.

5.3 代数扩域

从上一节我们看到,扩域 $F(\alpha)/F$ 的性质决定于 α 是 F 上的代数元还是超越元.本节我们要讨论,若集合 S 中的元都是 F 上的代数元,$F(S)$ 中元是否都是 F 上的代数元.

定义 E/F 为扩域,若 E 中任何元都是 F 上的代数元,我们称 E/F 为**代数扩域**.

定理 1 若 E/F 为有限扩域,则 E/F 为代数扩域.

证明 任取 $\alpha \in E$.我们要证明 α 是 $F[x]$ 内某多项式的根.由于 E/F 为有限扩域,即 E 作为 F 上的向量空间,维数$[E:F] = n$ 有限.于是,E 中 $n+1$ 个向量 $1,\alpha,\alpha^2,\cdots,\alpha^n$ 在 F 上线性相关,从而存在 F 中不全为 0 的 $b_0,b_1,\cdots,b_n$ 使

$$b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0,$$

即 α 为 $F[x]$ 中多项式 $f(x) = b_0 + b_1x + \cdots + b_nx^n$ 的根.

推理 1 若 $F(\alpha)/F$ 为单代数扩域,则 $F(\alpha)/F$ 为代数扩域.

证明 由于$[F(\alpha):F]$ 有限,由上述定理知命题为真.

推理 2 若 $E = F(\alpha_1,\cdots,\alpha_n)$,且 $\alpha_1,\cdots,\alpha_n$ 都是 F 上的代数元,则 E/F 为代数扩域.

证明 我们仅在 $n = 2$ 时,说明证明原理.由于

$$F \subset F(\alpha_1) \subset E = F(\alpha_1)(\alpha_2), F[x] \subset F(\alpha_1)[x],$$

故 α_2 也是 $F(\alpha_1)$ 上的代数元,从而我们有两个单代数扩域

$$F(\alpha_1)(\alpha_2)/F(\alpha_1), \quad F(\alpha_1)/F.$$

于是，

$$[E:F]=[F(\alpha_1)(\alpha_2):F(\alpha_1)][F(\alpha_1):F]$$

有限，从而 E/F 为代数扩域.

定理 2 若集合 S 中的元都是域 F 上的代数元，则 $F(S)/F$ 是代数扩域.

证明 由 5.1 的定理 3，若 $\beta\in F(S)$，则存在 $s_1,\cdots,s_n\in S$ 使

$$\beta=\frac{f(s_1,\cdots,s_n)}{g(s_1,\cdots,s_n)},$$

这里 $f(s_1,\cdots,s_n),g(s_1,\cdots,s_n)\in F[s_1,\cdots,s_n]\subset F(s_1,\cdots,s_n)$.从而

$$\beta\in F(s_1,\cdots,s_n).$$

再由上述的推论 2 知 β 为 F 上的代数元.总之，$F(S)/F$ 是代数扩域.

习题 5－3

1.令 E/F 为代数扩域，而 α 是 E 上的一个代数元.证明 α 是 F 上的一个代数元.

2.令 E/F 为有限扩域.证明存在 E 上的有限个元 $\alpha_1,\cdots,\alpha_m$，使

$$E=F(\alpha_1,\cdots,\alpha_m).$$

3.令 F,I,E 为域，且 $F\subset I\subset E$.假定 $[I:F]=m$，$\alpha\in E$ 在 F 上的次数为 n，而且 $(m,n)=1$.证明，α 在 I 上的次数也为 n.

4.令域 F 的特征不是 2，E/F 为扩域，且 $[E:F]=4$.证明：存在一个满足条件 $F\subset I\subset E$ 的 F 的二次扩域 $I\Leftrightarrow E=F(\alpha)$，且 α 在 F 上的极小多项式为 x^4+ax^2+b.

5.4 多项式的分裂域

1 多项式的分裂域

代数学中有一个重要的定理——代数学基本定理，即复数域 **C** 上的任何一个一元多项式在复数域 **C** 中至少有一个根，换个说法为，$\mathbf{C}[x]$ 中每个一元多项式在 $\mathbf{C}[x]$ 中都可分解成一次因式的乘积.进一步，这说明复数域 **C** 不再有真(比复数域大的)代数扩域了，我们称这样的域为代数闭域.事实上，用超限归纳可证实任何一个域都有一个代数扩域.这个结论的证明超出了本书的范围.但多项式分裂域的理论在一定意义下弥补了这一点.

定义 令 F 为域，$f(x)$ 为 F 上的首 1 的 $n(n\geqslant1)$ 次多项式.扩域 E/F 称为 $f(x)$ 在 F 上的**分裂域**，若

(1) $E=F(\alpha_1,\cdots,\alpha_n)$；

(2) $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$.

例1 $Q(\sqrt{2})/Q$ 为 x^2-2 的分裂域;$Q(\sqrt{2},\sqrt{3})/Q$ 为 $(x^2-2)(x^2-3)$ 的分裂域;C/R 为 x^2+1 的分裂域.

定理1 域 F 上的任何一个 $n(n\geq 1)$ 次首1多项式 $f(x)$ 都有一个分裂域 E/F.

证明 我们对多项式的次数用归纳法.

(1) 次数为1时,E/F 为所求.

(2) 假设定理命题对于 $n-1$ 次首1多项式成立.

(3) 设首1的 n 次多项式

$$f(x)=g(x)h(x),$$

这里 $g(x),h(x)\in F[x]$,$g(x)$ 首1,且不可约.此时,我们知道,存在一个单扩域 $F(\alpha_1)/F$,α_1 是 $g(x)$ 的根.此时,在 $F(\alpha_1)[x]$ 内 $f(x)=(x-\alpha_1)f_1(x)$,$f_1(x)$ 为 $F(\alpha_1)$ 上的 $n-1$ 次首1多项式.由归纳假设,存在 $f_1(x)$ 在 $F(\alpha_1)$ 上的分裂域 $E/F(\alpha_1)$,即

$$E=F(\alpha_1)(\alpha_2,\cdots,\alpha_n)=F(\alpha_1,\cdots,\alpha_n),f_1(x)=(x-\alpha_2)\cdots(x-\alpha_n).$$

此时,很明显 E/F 是 $f(x)$ 在 F 上的分裂域.

2 多项式的重根

定理3 令 $f(x)\in F[x]$ 为首1多项式,$f(x)$ 在其任何一个分裂域 E/F 内没有重根 $\Leftrightarrow$ 在 $F[x]$ 内 $(f(x),f'(x))=1$.

证明 首先,在 $F[x]$ 内 $(f(x),f'(x))=1\Leftrightarrow$ 在 $E[x]$ 内 $(f(x),f'(x))=1$ 是明显的,因为 $F[x]\subset E[x]$.

$(\Rightarrow)$ 设在 $E[x]$ 内

$$f(x)=(x-r_1)\cdots(x-r_n),r_i\neq r_j(i\neq j),$$

则

$$f'(x)=\sum_i(x-r_1)\cdots(x-r_{i-1})(x-r_{i+1})\cdots(x-r_n)$$
$$\Rightarrow(x-r_i)\nmid f'(x),$$

从而 $(f(x),f'(x))=1$;

$(\Leftarrow)$ 若 $(x-r_i)^2\mid f(x)$,则

$$(x-r_i)\mid f'(x),\quad (f(x),f'(x))\neq 1.$$

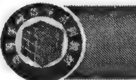
约定:以后我们说域 F 上的一个多项式有没有重根,是指在它的任何一个分裂域内它是否有相同的根.

定理4 令 $f(x)\in F[x]$ 为首1不可约多项式,则有如下结论:

(1) 当 $\mathrm{ch}F=0$ 时,$f(x)$ 没有重根;

(2) 当 $\mathrm{ch}F=p\neq 0$ 时,$f(x)$ 有重根 $\Leftrightarrow f(x)=g(x^p),g(x)\in F[x]$.

证明 由定理3,$f(x)$ 有重根 $\Leftrightarrow(f(x),f'(x))\neq 1$.而当 $f(x)$ 为不可约时,这等同于

$f(x)\mid f'(x)$，进而等同于 $f'(x)=0$.

(1) 当 $\mathrm{ch}F=0$ 时，且 $f(x)$ 不可约时，$f'(x)\neq 0$，即 $f(x)$ 没有重根；

(2) 当 $\mathrm{ch}F=p\neq 0$ 时，若 $f(x)=a_0+a_1x\cdots+a_nx^n$，则

$$f'(x)=a_1+2a_2x+\cdots+(n-1)a_{n-1}x^{n-2}+na_nx^{n-1}=0$$
$$\Leftrightarrow a_1=2a_2=\cdots=na_n=0$$
$$\Leftrightarrow a_i=0\quad(p\nmid i;\ i=1,\cdots,n)$$

从而

$$f(x)=a_0+a_px^p+a_{2p}x^{2p}+\cdots+a_{tp}x^{tp}=g(x^p).$$

习题 5－4

1. 证明 x^4+1 在 $\mathbf{Q}$ 上的分裂域是单扩域 $\mathbf{Q}(\alpha)$，其中 $\alpha^4+1=0$.

2. 令 x^3-a 是域 $\mathbf{Q}$ 上的一个不可约多项式，β 是 x^3-a 的根. 证明 $\mathbf{Q}(\beta)$ 不是 x^3-a 在 $\mathbf{Q}$ 上的分裂域.

3. 令 $p_1(x),\cdots,p_m(x)$ 为域 F 上的 m 个首 1 的不可约多项式. 证明存在 F 的一个有限扩域 $E=F(\alpha_1,\cdots,\alpha_m)$，其中 α_i 在 F 上的极小多项式为 $p_i(x)$.

4. 令 F 为特征为素数 p 的域，$E=F(\beta)$，β 是 $F[x]$ 中多项式 x^p-a 的根. $F(\beta)/F$ 是不是 x^p-a 的分裂域？

5. 令 F 为特征 $p(\neq 0)$ 的域，$a\in F$. 证明：

(1) $f(x)=x^p-x-a$ 没有重根；

(2) $f(x)$ 在 $F[x]$ 内不可约 $\Leftrightarrow f(x)$ 在 F 内没有根. *

6. 令 $p_1(x),p_2(x)\in F[x]$ 为两个不同的首 1 不可约多项式，且 $p_1(x),p_2(x)$ 没有重根. 求证，多项式 $f(x)=p_1(x)p_2(x)$ 也没有重根. *

5.5 有 限 域

定义 元的个数有限的域称为有限域.

例如，当 p 为素数时，$\mathbf{Z}_p$ 为有限域，它的特征为 p.

定理 1 (1) 若 E 为特征为 p 的有限域，且有 q 个元素，Δ 为它的素域，$[E:\Delta]=n$，则：

① $q=p^n$；

② 域 E 是 Δ 上多项式 x^q-x 的分裂域；

③ 元数相同(特征相同)的任何两个有限域都同构.

(2) 对于任何素数 p 和任何正整数 n，存在有 $q=p^n$ 个元的有限域.

证明 (1) ① 令 $e_1,\cdots,e_n$ 为 E 在 Δ 上的基，则 E 中的每个元可唯一地表示为

$$\delta_1 e_1 + \cdots + \delta_n e_n,$$

因而 E 中元素的个数为 $q = p^n$.

② 因 E 的乘法群 E^* 有 $q-1$ 个元，故 $\alpha^{q-1} = 1(\alpha \in E^*)$.从而

$$\alpha^q = \alpha(\alpha \in E),$$

即 $\Delta[x]$ 中的多项式 $x^q - x$ 在 E 内有 q 个不同的根：$\alpha_1, \cdots, \alpha_q$，又

$$E = \Delta(\alpha_1, \cdots, \alpha_q)$$

是明显的.于是，E 是 Δ 上多项式 $x^q - x$ 的分裂域.

③ 这是 ② 的直接结果.

(2) 令 $E = \Delta(\alpha_1, \cdots, \alpha_q)$ 为 Δ 上多项式 $f(x) = x^q - x$ 的分裂域，$\alpha_1, \cdots, \alpha_q$ 是此多项式的全部根.首先，由于 $f'(x) = -1$，故 $f(x)$ 没有重根，即 $\alpha_1, \cdots, \alpha_q$ 互不相同.又由于

$$(\alpha_i - \alpha_j)^{p^n} = \alpha_i^{p^n} - \alpha_j^{p^n} = \alpha_i - \alpha_j,$$

$$(\alpha_i \alpha_j^{-1})^{p^n} = \alpha_i^{p^n}(\alpha_j^{p^n})^{-1} = \alpha_i \alpha_j^{-1}(\alpha_j \neq 0),$$

从而 $\{\alpha_1, \cdots, \alpha_q\}$ 为域，进而域 $E = \Delta(\alpha_1, \cdots, \alpha_q) = \{\alpha_1, \cdots, \alpha_q\}$ 有 $q = p^n$ 个元素.

评注：由于有 p^n 个元的有限域由 p^n 唯一决定，我们将其记为 $\mathbf{F}_{p^n}$

有限域除了上述的特点外，还有一个重要的性质，即有限域 E 是其素域 Δ 上的单扩域.为证明此结论，我们先给出一个有关有限交换群的一个结论.

引理　若 G 为有限交群，m 为 G 中元的阶的最大者，则 m 能被 G 的每个元的阶整除.

证明　首先，由第二章的习题 2 - 5 - 8 知，

$$a, b \in G, o(a) = k, o(b) = l, (k, l) = 1 \Rightarrow o(ab) = kl.$$

现在，假设 $c \in G, o(c) = n \nmid m$，则存在素数 p：

$$m = p^i m_1, p \nmid m_1;\quad n = p^j n_1, j > i.$$

令 $d \in G, o(d) = m$.于是，

$$a = d^{p^i} \text{ 的阶为 } m_1;\quad b = c^{m_1} \text{ 的阶为 } p^j.$$

由前述的结论，$o(ab) = p^j m_1 > m$，而这是矛盾的.

定理 2　有限域 E 是其素域 Δ 上的单扩域.

证明　设 E 有 q 个元，m 是它的乘法群 E^* 中元的最大的阶，则 $m \mid (q-1)$，从而 $m \leqslant q-1$. 由引理，

$$\alpha^m = 1\ (\alpha \in E^*),$$

这说明，多项式 $x^m - 1$ 至少有 $q-1$ 个不同的根.但由多项式的理论，在一个域中，一个多项式的不同的根的个数不会大于多项式的次数，因而 $q - 1 \leqslant m$. 总之，乘法群 E^* 中有一个元 α 的阶为 $q-1$.这就证明了

$$E = \Delta(\alpha).$$



习题 5 - 5

1.令 F 为有 p^n 个元的伽罗瓦域.证明，若 $n = km, m \geqslant 1$，则存在且仅存在 F 的一个子域有 p^m 个元素.

2.一个有限域一定有比它大的代数扩域.

3.将 $x^p - x$ 在 $\mathbf{Z}_p[x]$ 内分解成一次式的乘积.

4.找出 $\mathbf{Z}_2[x]$ 内的一切三次不可约多项式.

5.(1) 证明 $\mathbf{Z}_2[x]/I$ 为域,这里 $I = (x^3 + x^2 + 1)$；

(2) 选 $\alpha = x + I$,验证 $\mathbf{Z}_2[x]/I = \mathbf{Z}_2(\alpha)$,并以最简的 $f(x) + I$ 形式写出 $\mathbf{Z}_2[x]/I$ 的全部元素；

(3) 求证 $\mathbf{Z}_2[x]/I$ 为有 8 个元素；

(4) 对商环 $\mathbf{Z}_2[x]/(x^3 + x + 1)$,你有什么结论?

6.设 $p(x)$ 为 $\mathbf{F}_q$ 上的 n 次首 1 不可约多项式,$I = (P(x))$.求证：

(1) $p(x) \mid (x^{q^n} - x)$；

(2) $p(x)$ 没有重根.

第6章　格与布尔代数简介

本章中我们简单地介绍两个赋有序结构的代数结构——格和布尔代数.在计算机科学中它们有广泛的应用.

6.1　偏序集

1　偏序集

偏序集是本章的基础概念.首先,我们在第一章中定义了集合 A 上的关系为集合 $A\times A=\{(a,b)\mid a,b\in A\}$ 的一个非空子集.

定义　集合 A 的关系 $\leqslant$ 称为 A 上的一个**偏序关系**,若 $\leqslant$ 满足下列三个条件:

①$a\leqslant a(a\in A)$(**反身性**);

②$a\leqslant b,b\leqslant a\Rightarrow a=b$(**反对称性**);

③$a\leqslant b,b\leqslant c\Rightarrow a\leqslant c$(**传递性**).

一个赋有偏序关系 $\leqslant$ 的集合 A 称为**偏序集**,记为$(A,\leqslant)$.

为方便,当 $a\leqslant b$ 时,我们称"a **小于等于** b";也将 $a\leqslant b$ 写成 $b\geqslant a$,称"b **大于等于** a".若 $a\leqslant b$,但 $a\neq b$,记为 $a<b$,称"a 小于 b".

例1　设 S 为任何一个集合,$p(S)$ 为 S 的一切子集构成的集合,$X\leqslant Y$ 表示集合 X 为集合 Y 的子集,即 $X\subseteq Y$,则$(p(S),\leqslant)$为偏序集.$\leqslant$ 满足上述三条是明显的.

例2　若 $a\leqslant b$ 就是整数的小于或等于关系,则$(\mathbf{Z},\leqslant)$也是偏序集.

例3　若 $a<b$ 就是整数的小于关系,则$(\mathbf{Z},<)$不是偏序集,因为①不成立.

例4　若 A 为正整数构成的非空集合,$a\mid b$ 表示 a 是 b 的因子,$a\parallel b$ 表示 a 是 b 的倍数,则$(A,\mid)$和$(A,\parallel)$都是偏序集.

全序集:$(A,\leqslant)$为偏序集,A 中的两个元素 a,b 称为**可比较的**,若 $a\leqslant b$ 或 $b\leqslant a$ 成立.若 A 中任何两个元素都可比较,我们称$(A,\leqslant)$为**全序集**或称 A 是**线性序**的,此时也可称 A 是一个**链**.

例如,当 $S=\{0,1\}$ 时,偏序集$(p(S),\leqslant)$不是链,因为$\{0\}$和$\{1\}$不可比较.$(\mathbf{Z},\leqslant)$是全序集.事实上,$\mathbf{Z}$ 中的全部元素可用 $\leqslant$ 链结起来: $\cdots\leqslant-2\leqslant-1\leqslant0\leqslant1\leqslant2\leqslant\cdots$.



2　哈氏(Hasse)图

在偏序集 A 中，我们用图 6-1 的哈氏图表示 $a<b$.



图 6-1

例 5　当 $A=\{a\}, B=\{a,b\}, C=\{a,b,c\}$ 时，偏序集 $(p(A),\leqslant)$, $(p(B),\leqslant)$ 和 $(p(C),\leqslant)$ 的哈氏图分别如图 6-2:

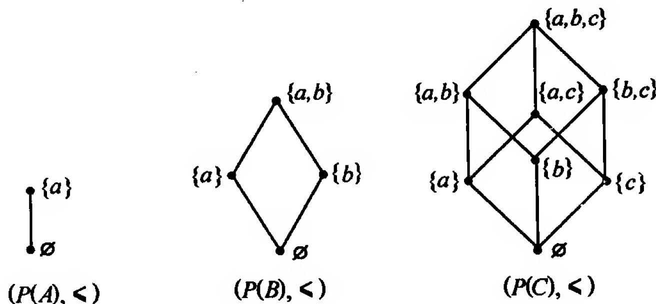


图 6-2

例 6　当 $A=\{2,3,4,5,15,60\}$ 时，偏序集 $(A,\mid)$ 和 $(A,\parallel)$ 的哈氏图如图 6-3:

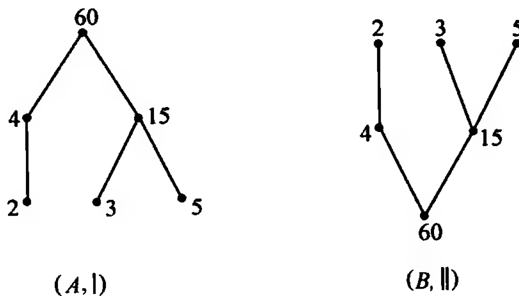


图 6-3

3　偏序集的同构

与其它代数结构一样，有时我们也要比较两个偏序集的结构，因而我们也要定义偏序集的同态和同构，对于偏序集，有意义的是同构.

定义　说两个偏序集 $(A,\leqslant)$ 与 $(B,\leqslant')$ 同构是指存在一个由 A 到 B 的保序双射 $\sigma: a\leqslant b\Rightarrow\sigma(a)\leqslant'\sigma(b)$.

例 7 (1)$\sigma: a \to a+1$ 是偏序集$(\mathbf{Z}, \leqslant)$的一个自同构;

(2) 偏序集$(p(\{a,b\}), \leqslant)$与$(\{1,2,3,6\}, |)$同构,同构为

$$\sigma: \varnothing \mapsto 1, \{a\} \mapsto 2, \{b\} \mapsto 3, \{a,b\} \mapsto 6.$$

4 偏序集中的端元

极小元:若 $a \in A$,且不存在 $c \in A$ 使$c < a$,称 a 为A 的**极小元**.

例 6 中,2,3,5 是$(A, |)$中的极小元.

极大元:若 $a \in A$,且不存在 $c \in A$ 使$a < c$,称 a 为A 的**极大元**.

例 6 中,2,3,5 是$(A, \|)$中的极大元.

最小元:若 $a \in A$,且对所有 $x \in A$ 有$a \leqslant x$,称 a 为A 的**最小元**.

例 6 中,60 是$(A, \|)$中的最小元.

最大元:若 $a \in A$,且对所有 $x \in A$ 有 $x \leqslant a$,称 a 为 A 的**最大元**.

例 6 中,60 是$(A, |)$中的最大元.

上界和下界:若 $u \in A$,且对任何 $x \in S$ 有$x \leqslant u$,则称 u 为S 的(一个)**上界**;若 $d \in A$,且对任何 $x \in S$ 有$d \leqslant x$,则称 d 为S 的(一个)**下界**.

在例 6 的偏序集$(A, |)$中,15 和 60 都是$\{3,5\}$的上界;在偏序集$(A, \|)$中,15 和 60 都是$\{3,5\}$的下界.

最小上界和最大下界:若 u 为S 的上界,且对任何 S 任何上界v,有 $u \leqslant v$,则称 u 为S 的**最小上界**,即上界当中的最小者;若 d 为S 的下界,且 S 的任何下界c 有$c \leqslant d$,则称 d 为S 的**最大下界**,即下界当中的最大者.

在例 6 的偏序集$(A, |)$中,15 是$\{3,5\}$的最小上界;在偏序集$(A, \|)$中,15 是$\{3,5\}$的最大下界.

最小上界和最大下界是唯一的.

在偏序集$(p(S), \leqslant)$中,$A \cup B$ 是$\{A,B\}$的最小上界;$A \cap B$ 是$\{A,B\}$的最大下界.仿此,在一个偏序集中,我们用 $a \vee b$ 表示$\{a,b\}$的最小上界,称为 **a,b 的并**;用 $a \wedge b$ 表示$\{a,b\}$的最大下界,称为 **a,b 的交**.

习题 6-1

1.判断 A 上的关系 R 是否为偏序关系:

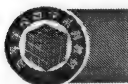
(1)$A = \mathbf{Z}, aRb \Leftrightarrow a = 2b$;

(2)$A = \mathbf{Z}, aRb \Leftrightarrow b^2 | a$;

(3)$A = \mathbf{Z}, aRb \Leftrightarrow a = b^k$(对某个 $k > 0$).

2.令 $A = \{a,b,c\}$.找出 A 上满足$a \leqslant b$ 的一切偏序关系.

3.令 $A = \{1,2,3,5,6,10,15,30\}, S = \{a,b,c\}$.求证$(A, |)$与$(p(S), \leqslant)$同构.



6.2 格

1 格

有上一节的准备,现在我们可以定义格这个新的代数结构了.

定义 (1) 若一个偏序集中任何两个元素都有最小上界和最大下界,则我们称此偏序集为格.

(2) L 为格,S 是 L 的非空子集.若对任何 $a,b\in S$,有 $a\vee b,a\wedge b\in S$,则我们称 S 是 A 的子格.

格同构的特点:若 $\sigma:L_1\to L_2$ 为格同构,很明显有

$$\sigma(a\vee b)=\sigma(a)\vee\sigma(b),\quad \sigma(a\wedge b)=\sigma(a)\wedge\sigma(b).$$

例 1 对于任何集合 S,$(p(S),\leqslant)$ 是一个格,且

$$A\vee B=A\cup B,\quad A\wedge B=A\cap B.$$

例 2 $(\mathbf{Z}^+,|)$ 是一个格,对于任何正整数 a,b,$a\vee b$ 是 a,b 的最小公倍数,$a\wedge b$ 是 a,b 的最大公因子.

例 3 若 $n\in\mathbf{Z}^+$,我们用 D_n 表示 n 的一切正因子的集合,则 $(D_n,|)$ 是 $(\mathbf{Z}^+,|)$ 的子格.D_{20} 和 D_{30} 的哈氏图如图 6-4.由哈氏图,我们不难看出格 D_{30} 与 $p(\{a,b,c\})$ 同构.

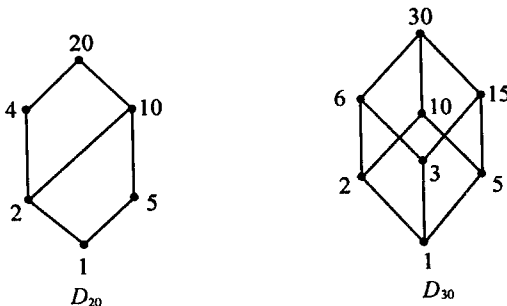


图 6-4

2 格的基本性质

在讨论格的基本性质前,我们简单重申 $a\vee b$ 和 $a\wedge b$ 的含义:

(1) $a\leqslant a\vee b,b\leqslant a\vee b$; $a\vee b$ 是 a,b 的最小上界;

(2) 若 $a\leqslant c,b\leqslant c$,则 $a\vee b\leqslant c$;

(3) $a\wedge b\leqslant a,a\wedge b\leqslant b$; $a\wedge b$ 是 a,b 的最大下界;

(4) 若 $c \leqslant a, c \leqslant b$，则 $c \leqslant a \wedge b$.

定理 1 设 L 为格，则下列各项成立：

(1) $a \vee b = b \Leftrightarrow a \leqslant b$;

(2) $a \wedge b = a \Leftrightarrow a \leqslant b$;

(3) $a \wedge b = a \Leftrightarrow a \vee b = b$.

证明 (1) 令 $a \vee b = b$. 由于 $a \leqslant a \vee b$，故 $a \leqslant b$. 反之，令 $a \leqslant b$. 由于 $b \leqslant b$，故 b 是 $\{a, b\}$ 的一个上界，从而 $a \vee b \leqslant b$. 但我们有 $b \leqslant a \vee b$. 于是，$a \vee b = b$.

(2) (2) 的证明与 (1) 的证明类似，留给读者练习.

(3) (1) 和 (2) 的直接结果.

定理 2 设 L 为格，则下列各项成立：

(1)（**幂等律**）

$$a \vee a = a, \quad a \wedge a = a;$$

(2)（**交换律**）

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a;$$

(3)（**结合律**）

$$(a \vee b) \vee c = a \vee (b \vee c),$$
$$(a \wedge b) \wedge c = a \wedge (b \wedge c);$$

(4)（**吸收律**）

$$(a \vee b) \wedge a = a, \quad (a \wedge b) \vee a = a.$$

证明 (1) 由最小上界和最大下界的定义，这是明显的.

(2) 理由同上.

(3) 我们仅证明 $(a \vee b) \vee c = a \vee (b \vee c)$. 另一个的证明留给读者. 首先，我们有 $a \leqslant a \vee (b \vee c), b \vee c \leqslant a \vee (b \vee c)$. 又 $b \leqslant b \vee c, c \leqslant b \vee c$. 由传递性，我们得到

$$b \leqslant a \vee (b \vee c), c \leqslant a \vee (b \vee c)$$

于是，$a \vee b \leqslant a \vee (b \vee c)$. 进而，

$$(a \vee b) \vee c \leqslant a \vee (b \vee c).$$

类似地，我们可得到 $(a \vee b) \vee c \geqslant a \vee (b \vee c)$. 由反对称性，我们可得到

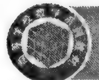
$$(a \vee b) \vee c = a \vee (b \vee c).$$

(4) 我们仅证明 $(a \vee b) \wedge a = a$. 另一个的证明留给读者. 首先，$(a \vee b) \wedge a \leqslant a$ 是明显的. 另一方面，$a \vee b \geqslant a, a \geqslant a$，故 $(a \vee b) \wedge a \geqslant a$. 再由反对称性，我们可得到

$$(a \vee b) \wedge a = a.$$

评注：因为格中的运算 $\vee$ 和 $\wedge$ 满足结合律，所以在格中，集合 $\{a_1, \cdots, a_n\}$ 的最小上界和最大下界分别为 $a_1 \vee \cdots \vee a_n$ 和 $a_1 \wedge \cdots \wedge a_n$.

定理 3 设 L 为格，则下列各项成立：



(1)$a \leqslant b \Rightarrow a \vee c \leqslant b \vee c$, $a \wedge c \leqslant b \wedge c$;

(2)$a \leqslant c, b \leqslant c \Leftrightarrow a \vee b \leqslant c$;

(3)$c \leqslant a, c \leqslant b \Leftrightarrow c \leqslant a \vee b$;

(4)$a \leqslant b, c \leqslant d \Rightarrow a \vee c \leqslant b \vee d$, $a \wedge c \leqslant b \wedge d$.

证明 证明留给读者.

以上我们仅指出了格的一些基本性质.在实际中,我们所关注的是具备一些优良性质的格.以下我们介绍几种特殊的格.

3 有界格

定义 若一个格 L 有一个最大元 1 和一个最小元 0,则我们称 L 是**有界格**.

例 4 $(p(S), \leqslant)$ 是有界格,最大元为 $1 = S$,最小元为 $0 = \varnothing$.

例 5 $(D_n, |)$ 是有界格,最大元为整数 n,最小元为整数 1.

例 6 $(\mathbf{Z}^+, |)$ 不是有界格,它有最小元,但没有最大元.

$$1 = a_1 \vee \cdots \vee a_n, 0 = a_1 \wedge \cdots \wedge a_n.$$

定理 4 有限格 $L = \{a_1, \cdots, a_n\}$ 是有界的.

证明 $1 = a_1 \vee a_2 \cdots a_n$, $0 = a_1 \wedge a_2 \cdots \wedge 2a_n$.

4 分配格

定义 若格 L 满足下面的**分配律**,则我们称 L 是**分配格**:

(1)$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

(2)$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

例 7 $(p(S), \leqslant)$ 是分配格,这是因为对于 S 的子集 A, B, C 我们有:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

例 8 求证下面两个哈氏图(如图 6 - 5)表示的格不是分配格:

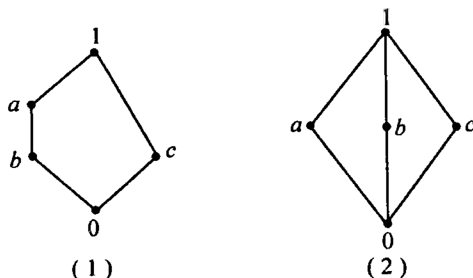


图 6 - 5

证明 (1) 我们有 $a \wedge (b \vee c) = a \wedge 1 = a$,但

$$(a \wedge b) \vee (a \wedge c) = b \vee 0 = b;$$

(2) 我们同样有 $a \wedge (b \vee c) = a \wedge 1 = a$,但

$$(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0.$$

5 补格

补元:在一个有界格 L 中,若 $a \vee a' = 1, a \wedge a' = 0$,则我们称 a, a' 互补,也称 a' 为 a 的补元.

定义 若一个有界格 L 中的每个元都有补元,则我们称 L 是**有补格**.

例 9 $(p(S), \leqslant)$ 和 $(D_{30}, |)$ 是有补格:$p(S)$ 中,每个元都有补元,A 的补元 $A' = S - A$;$(D_{30}, |)$ 中的每个元都有补元,例如,$5' = 6$,因为 $5 \vee 6$ 为 30,$5 \wedge 6$ 为整数 1.$(D_{20}, |)$ 不是有补格:在 D_{20} 中,2,10 没有补元.

习题 6-2

1.令 $A = \{2,3,6,12,24,36,72\}$.偏序集 $(A, |)$ 是格吗?

2.证明,若 a, b 为有界、分配格中的元素,a' 为 a 的补,则

$$a \vee (a' \wedge b) = a \vee b, \quad a \wedge (a' \vee b) = a \wedge b.$$

3.判断下列哈氏图(如图 6-6)表示的是否为格:

4.令 L 为分配格.证明,若存在 a 使

$$a \vee x = a \vee y, \quad a \wedge x = a \wedge y,$$

则 $x = y$.

5.令 L 为至少有两个元的有界格.求证在 L 中不存在 a 使

$$a = a'.$$

6.3 布尔代数

1 布尔代数

定义 我们称一个有界的、分配的有补格为**布尔代数**.

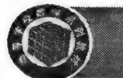
在计算机科学中,应用最广泛的是有限布尔代数,即元素个数有限的布尔代数.

例 1 对于任何集合 S,$(p(S), \leqslant)$ 是布尔代数.事实上,$p(S)$ 是布尔代数的原型.

定理 1 布尔代数 B 中,每个元 a 的补元 a' 是唯一的.

证明 令 a_1, a_2 都是 a 的补元,即

$$a \vee a_1 = 1, a \wedge a_1 = 0; \quad a \vee a_2 = 1, a \wedge a_2 = 0.$$



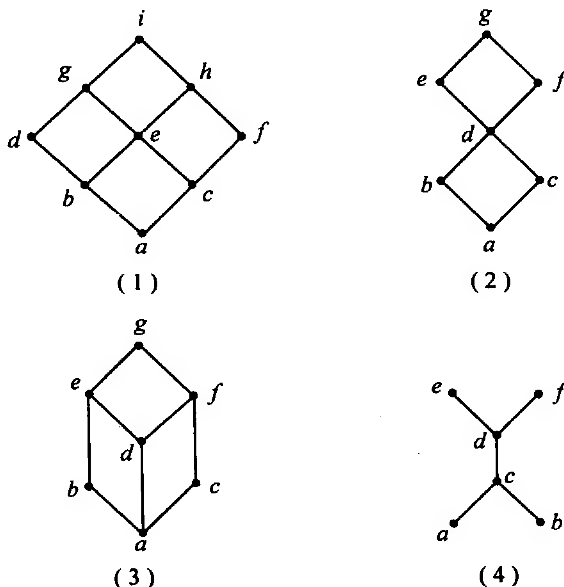


图 6-6

由此,我们得到

$$a_1 = a_1 \wedge 1 = a_1 \wedge (a \vee a_2) = (a_1 \wedge a) \vee (a_1 \wedge a_2)$$
$$= 0 \vee (a_1 \wedge a_2) = a_1 \wedge a_2,$$
$$a_2 = a_2 \wedge 1 = a_2 \wedge (a \vee a_1) = (a_2 \wedge a) \vee (a_2 \wedge a_1)$$
$$= 0 \vee (a_2 \wedge a_1) = a_2 \wedge a_1,$$

因而 $a_1 = a_1 \wedge a_2 = a_2 \wedge a_1 = a_2$.

定理 2(布尔代数的替换法则) 当将 $\cup$, $\cap$ 对应改为 $\vee$, $\wedge$ 后,布尔代数$(p(S), \leqslant)$中由 $\cup$, $\cap$ 表示的运算律在任何布尔代数中也成立,特别有:

(1)**(对合律)** $(a')' = a$;

(2)**(德·摩根律)** $(a \vee b)' = a' \wedge b'$,

$(a \wedge b)' = a' \vee b'$.

证明 我们不去逐一证明此结论.仅将上述两个运算律的证明留给读者练习.

评注:我们是从序的角度定义布尔代数的,但我们看到 $\vee$, $\wedge$ 为布尔代数上的两个二元运算,$'$ 为一元运算.序关系与运算 $\vee$, $\wedge$ 的互换关系为 $a \leqslant b \Leftrightarrow a \vee b = b$ 或 $a \leqslant b \Leftrightarrow a \wedge b = a$.运算 $\vee$, $\wedge$ 和 $'$ 满足许多常见的运算律,特别是下面的运算律:

(1)(**交换律**)

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a.$$

(2)(**分配律**)

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

(3)(**幺律**)

$$a \vee 0 = a, \quad a \wedge 1 = a.$$

(4)(**互补律**)

$$a \vee a' = 1, \quad a \wedge a' = 0.$$

事实上，我们可以从运算的角度定义一个布尔代数是代数结构，其具备三个运算 $\vee$，$\wedge$ 和 $'$，且它们满足上述 4 项运算律，布尔代数的其它运算律可由这 4 项推出. 因而，我们也用 $(B, \vee, \wedge, ')$ 表示布尔代数 B.

2　布尔环

历史上讲，布尔代数是由英国数学家 Boole 用来形式化命题运算的. 长久以来，被认为它与一般代数结构(如群，环，域)不同，但后来 Stone 证实布尔代数本质上可以视为一个环，即由布尔代数我们能构造一个环 —— 布尔环.

定义　一个有单位元 1 的环称为**布尔环**，若它的元都是**幂等的**，即 $a^2 = a$.

布尔环实际上是交换环，这由下面的运算可以看出：

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + (ab + ba) \Rightarrow ab + ba = 0,$$
$$2a = 2a^2 = aa + aa = 0 \Rightarrow a = -a,$$
$$ab = -ba = ba.$$

评注：由上述运算可以看出，布尔环 B 的加群 $(B, +)$ 中每个非零元的阶为 2，故可视其为有限域 $\mathbf{F}_2$ 上的线性空间.

事实上，布尔代数和布尔环是等价的，即由一个布尔代数可构造一个布尔环. 反之，由一个布尔环也可构造一个布尔代数，且相互间是唯一确定的. 在此我们仅指出由布尔代数造布尔环的过程.

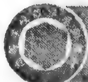
定理 3　设 B 为布尔代数，1 为最大元，0 为最小元. 对任何 a, b，我们规定：

$$a + b \equiv (a \wedge b') \wedge (a' \wedge b) \quad (a, b \text{ 的}\textbf{对称差}),$$
$$a \cdot b \equiv a \wedge b,$$

则代数结构 $(B, +, \cdot)$ 为布尔环，1 为单位元，0 为零元.

证明　我们可以按环的定义逐一验证 $(B, +, \cdot)$ 满足环的定义，但这是一个很繁琐的过程，我们仅说明加法的结合律，其它各项可同样得到验证.

首先我们指出，由 $a + b$ 和 $a \cdot b$ 的定义，我们很容易证明：



(1) $a' = 1 + a$;

(2) $a + b = (a \vee b) \wedge (a \wedge b)'$;

(3) $a \vee b = a + b - ab$

在布尔代数 $p(S)$ 中，A,B 的对称差 $A + B$ 就是图 6－7 中阴影部分.

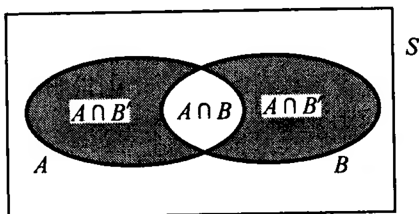


图 6－7

由此，

$$(a + b)' = [(a \vee b) \wedge (a \wedge b)']'$$
$$= (a \vee b)' \vee (a \vee b) = (a \wedge b) \vee (a' \wedge b').$$

$$(a + b) + c = [(a + b) \wedge c'] \vee [(a + b)' \wedge c]$$
$$= [((a \wedge b') \vee (a' \wedge b)) \wedge c'] \vee [((a \wedge b) \vee (a' \wedge b')) \wedge c]$$
$$= [(a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')] \vee [(a \wedge b \wedge c) \vee (a' \wedge b' \wedge c)]$$
$$= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b' \wedge c)$$

此式中，a,b,c 是对称的，因而

$$(a + b) + c = a + (b + c).$$

3　有限布尔代数的原子表示

布尔代数的原子：我们称布尔代数中的非零极小元为原子.

有限布尔代数中的原子就是哈氏图中紧位于零元之上的元素.例如，若 $S = \{a_1, a_2, \cdots, a_n\}$，则 $\{a_1\},\{a_2\},\cdots,\{a_n\}$ 为布尔代数 $p(S)$ 的 n 个原子.我们注意 $p(S)$ 的每个非零元都可唯一地表示成若干原子 $\{a_1\},\{a_2\},\cdots,\{a_n\}$ 的并.我们将证明，对于任何有限布尔代数这个结论也成立.

定理 4　设 B 为有限布尔代数，则 B 中元素的个数为 2^n，B 有 n 个原子，且每个非零元都可唯一地表示成若干个原子的并(不记次序).

证明　令 $(B, +, \cdot)$ 为上述构造的布尔环.视 $(B, +)$ 为有限域 $\mathbf{F}_2$ 上的线性空间，设其维数为 n，且 $e_1, e_2, \cdots, e_n$ 为基底，则

$$B = \{k_1 e_1 + k_2 e_2 + \cdots + k_n e_n \mid k_i = 0,1 (i = 1,2,\cdots,n)\},$$

从而我们得知 B 有 2^n 个元素.

另一方面,当 $e_i \neq e_j$ 时,B 的子布尔代数

$$\{e_i \wedge e_j, e_i, e_j, e_i \vee e_j\}$$

明显为 e_i, e_j 的线性组合 $\{0, e_i, e_j, e_i + e_j\}$,故 $e_i \wedge e_j = 0$, 从而

$$e_i \vee e_j = e_i + e_j - e_i \wedge e_j = e_i + e_j.$$

上式说明 $e_1, e_2, \cdots, e_n$ 为布尔代数 B 的原子, 且

$$B = \{k_1 e_1 \vee k_2 e_2 \vee \cdots \vee k_n e_n \mid k_i = 0,1(i = 1,2,\cdots,n)\}.$$

评注:令 $S = \{e_1, e_2, \cdots, e_n\}$, 则上述的布尔代数 B 同构于 $p(S)$.从而,本质上讲,有限布尔代数仅 $p(S)$ 一种.由上面的证明我们看到

$$\sigma: A \longmapsto \sum_{e \in A} e$$

为 $p(S)$ 到 B 的双射.事实上,很容易证明 σ 保持运算.为清晰,我们举例说明.例如,取 $A = \{e_1, e_2, e_3\}, B = \{e_2, e_3, e_4, e_5\}$.此时,在 $p(S)$ 中,

$$A \cup B = \{e_1, e_2, e_3, e_4, e_5\}, \quad A \cap B = \{e_2, e_3\};$$

在 B 中,

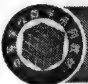
$$\begin{aligned}
\sigma(A) \vee \sigma(B) &= (\sum_{e \in A} e) \vee (\sum_{e \in B} e) \\
&= (e_1 + e_2 + e_3) \vee (e_2 + e_3 + e_4 + e_5) \\
&= (e_1 \vee e_2 \vee e_3) \vee (e_2 \vee e_3 \vee e_4 \vee e_5) \\
&= e_1 \vee e_2 \vee e_3 \vee e_4 \vee e_5 \\
&= \sigma(\{e_1, e_2, e_3, e_4, e_5\}) \\
&= \sigma(A \cup B); \\
\sigma(A) \wedge \sigma(B) &= (\sum_{e \in A} e) \wedge (\sum_{e \in B} e) \\
&= (e_1 + e_2 + e_3) \wedge (e_2 + e_3 + e_4 + e_5) \\
&= (e_1 + e_2 + e_3) \cdot (e_2 + e_3 + e_4 + e_5) \\
&= e_2 + e_3 \\
&= \sigma(A \cap B) \\
&\{e_i^2 = e_i, e_i \cdot e_j = 0\ (i \neq j)\}.
\end{aligned}$$

习题 6 – 3

1.判断下列哈氏图(如图 6 – 8) 表示的偏序集是否为布尔代数:

2.证明,在布尔代数中,$a \leqslant b \Leftrightarrow b' \leqslant a'$.

3.证明, 在布尔代数中,$a = b \Leftrightarrow (a \wedge b') \vee (a' \wedge b) = 0$.



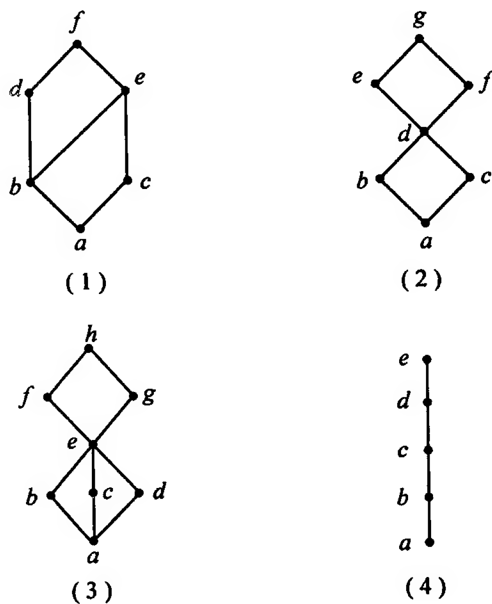


图 6 – 8

4.若$(B, +, \cdot)$是布尔代数$(B, \vee, \wedge)$,求证:

(1)$a' = 1 + a$;

(2)$a + b = (a \vee b) \wedge (a \wedge b)'$;

(3)$a \vee b = a + b - ab$.

第 7 章　应用举例

近世代数不仅在数学上有广泛的应用，在物理、化学、计算机学科等方面也有广泛而重要的应用.本章中，我们仅通过举例介绍近世代数在几个方面的简单应用，远不是近世代数应用的全面展示.事实上，对于许多专门的应用有专门深入的论著.本书参考文献 3 是介绍近世代数学及其应用的一般性书目. 若读者有兴趣，可参考此书.

7.1　Burnside 定理的应用

1　正多面体着色问题

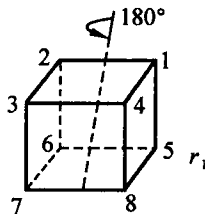
问题 1　用 n 种不同的颜色给一个正方体的 6 个面染色，问有多少种不同的染色法?

解　若固定正方体，6 个面中的每个都有 n 种不同的染色方式，共有 n^6 中染色法：$X=\{c_1,c_2,\cdots,c_{n^6}\}$.在这些染色法中，经过正方体的旋转，一种可成为另一种.令正方体的旋转群(旋转对称构成的)为 G，让 G 作用在 X 上，则不同染色法的个数就是 X 在 G 的作用下产生的轨道的个数.这样，我们就可以借助于 Burnside 定理解决问题.

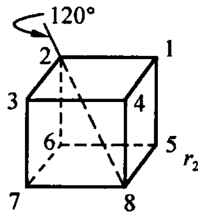
首先，我们说 $|G|=24$.我们将 G 作用在正方体的 8 个顶点上，对于每个顶点 x，轨道 Gx 中点的个数明显为 8；而 stab$x$ 的阶数为 3，因为固定 x 的旋转对称轮换与 x 相临的 3 个顶点.于是

$$|G|=|Gx|\cdot|\mathrm{stab}x|=8\times3=24.$$

见图 7－1，正方体的旋转群有如下 5 种类型的元素：



共1-2棱的两面同色
共7-8棱的两面同色
左右两面同色



共顶点2的三面同色
共顶点8的三面同色



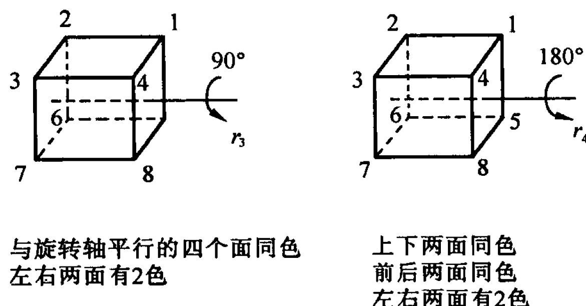


图 7－1

(1) 恒同 r_0,1 个：

可染 $c_0 = 6$ 种颜色在 r_0 之下不变；

(2) 绕过相对两棱中点之轴 180° 的旋转 r_1,此种有 6 个：

可染 $c_1 = 3$ 种颜色在 r_1 之下不变；

(3) 绕过相对两顶点之轴 120° 的旋转 r_2,此种有 8 个：

可染 $c_2 = 2$ 种颜色在 r_2 之下不变；

(4) 绕过相对两面中心轴 90° 的旋转 r_3,此种有 6 个：

可染 $c_3 = 3$ 种颜色在 r_3 之下不变；

(5) 绕过相对两面中心轴 180° 的旋转 r_4,此种有 3 个：

可染 $c_4 = 4$ 种颜色在 r_4 之下不变.

下表给出了在以上 5 种旋转下不变的染色法的个数,最后结果为：

$$\frac{1}{24}\sum_{g\in G}|F_g| = \frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2).$$

r	r 型的个数 s	颜色数 c	$\|F_r\| = n^c$	$s\cdot\|F_r\|$
r_0	1	6	n^6	n^6
r_1	$6\times1=6$	3	n^3	$6n^3$
r_2	$4\times2=8$	2	n^2	$8n^2$
r_3	$3\times2=6$	3	n^3	$6n^3$
r_4	$3\times1=3$	4	n^4	$3n^4$
			$\|G\| = 24$	$\sum = n^6+3n^4+12n^3+8n^2$

2　开关线路的计数问题

开关线路由若干个开关 $A_1,\cdots,A_n$ 组成.一个开关线路也有接通(1)和断开(0)两个状态.在设计开关线路时,我们要考虑开关线路的等值问题.为了更清晰地说明原理,我们考虑一种简单的开关线路——由3个开关 A_1,A_2,A_3 构成的一个开关线路.我们可以将这样的开关线路视为一个黑匣子,其有3个二元输入端:x_1,x_2,x_3 和一个二元输出端:$f(x_1,x_2,x_3)$(见图7－2(1)).对于两个线路 f 和 g,若存在置换 $\pi\in S_3$ 使 $g(x_{\pi(1)},x_{\pi(2)},x_{\pi(3)})=f(x_1,x_2,x_3)$,则我们说这两个线路等值.即我们可以由两个等值线路的一个置换其外面的输入线而得到另一个(见图7－2(2)),此时我们可以视 π 为输入端转换器.

问题2　有三个开关,且不等值的开关线路有多少个?

解　因为输入端有8种选择,而输出有2种选择,故有 2^8 个可能的开关线路.令其集合为

$$X=\{f_1,f_2,\cdots,f_{2^8}\}.$$

我们将 S_3 自然地作用在 X 上:

$$(\pi*f)(x_1,x_2,x_3)=f(x_{\pi(1)},x_{\pi(2)},x_{\pi(3)}).$$

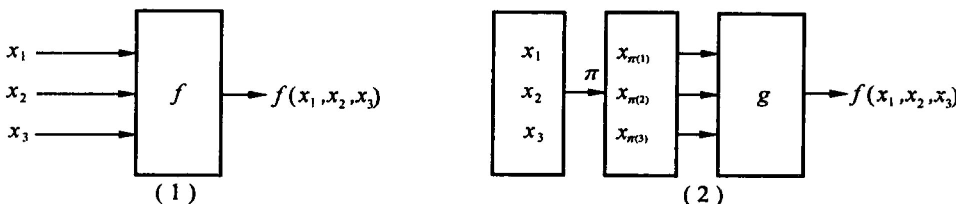


图7－2

这样,我们的问题等同于求作用轨道的个数.我们用Burnside定理解决此问题,为此我们要计算 S_3 中每个元在 X 中不动点的个数.例如,取 $\pi=(12)\in S_3$,此时,

$$(\pi*f)(x_1,x_2,x_3)=f(x_1,x_2,x_3)$$

相当于

$$f(x_2,x_1,x_3)=f(x_1,x_2,x_3).$$

这又等同于 $f(0,1,x_3)=f(1,0,x_3)$,即

$$f(0,1,0)=f(1,0,0)\text{ 和 }f(0,1,1)=f(1,0,1).$$

这说明,在 $f(x_1,x_2,x_3)$ 的8个输入中,除在(1,0,0)和(1,0,1)上的取值受限制外,其余6个上的取值任意,即

$$f(0,0,0),f(0,0,1),f(0,1,0),f(0,1,1),f(1,1,0),f(1,1,1)$$



不受限制.从而 $\pi=(12)$ 的不动点的个数为 2^6.同样可计算其它元的不动点的个数.总之,我们有下表:

$g\in S_3$	类型的个数 s	$\lvert F_g\rvert$	$s\cdot\lvert F_g\rvert$
(1) 型	1	2^8	$2^8=256$
对换型	3	2^6	$3\times 2^6=192$
三循环型	2	2^4	$2\times 2^4=32$
	$\lvert S_3\rvert=6$		$\sum=480$
不等值的开关线路的个数		$\frac{1}{\lvert S_3\rvert}\sum=\frac{480}{6}=80$	

事实上,群在计数方面有广泛的应用,限于篇幅本节仅举两例,读者可参见参考书目,如参考文献 3.

习题 7-1

1.用 3 颗同样的黑珠和 6 颗同样的白珠做项链,可做多少种项链?

2.用 n 种不同的颜色给一个正方体的 8 个顶点染色,问有多少种不同的染色法?

7.2 多项式编码原理

1 编码问题

信息依赖于数字通讯,许多重要场合传递的数字不可出错,但受设备、天气、操作等方面的影响,在数字传送过程中又难免不出错,如何解决这一问题呢?

解决此问题的第一个方法是判别所接受到的信息是否有错,若有错要求重发这一信息.为了接收者检验错误,可对待发的信息进行适当的加工.为此我们简述几个名词.

我们称一个 k 位二进制数码表示的信息为 **k 位信息码**.对每个信息码附加 $n-k$ 位用于检错的二进制数码构成一个 **n 位码词**.这种数码称 **(n,k)-码**.由信息码得到码词的过程称为**编码**;接收者收到码词后经过检错后取出信息的过程称为**译码**.

最简单的检错码的方法是奇偶检错码. 如下表,码词的设计是使码词的数字和为偶数:

信息码	码词
00	000
01	101
10	110
11	011

第二种方法是设计一种**纠错码**,使接收者能按事先确定的规则纠正收到信息中可能出现的错误.最简单的纠错码是重复码. 如下表,信息码被重复 3 次:

信息码	码词
0	000
1	111

接收者只要检查三位数字是否相同,不同时以多纠少.

编码问题就是设计更有效更可靠的检错码和纠错码.方法很多,有用群论方法设计的群码.下面我们简单地介绍多项式在这方面的应用 —— **多项式编码**.

2　多项式编码的方法

下面我们设计一种(n,k) - 码.

设待传送的信息码为

$$b_0 b_1 b_2 \cdots b_{k-1},$$

其对应的**信息码多项式**为

$$m(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{k-1} x^{k-1} \in \mathbf{Z}_2[x];$$

又设码词

$$a_0 a_1 a_2 \cdots a_{n-1}$$

对应的**码词多项式**为

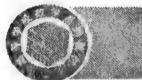
$$w(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \in \mathbf{Z}_2[x].$$

现在,我们给出一个方法将每个信息码多项式按一定的规则得到码词多项式,即将每个信息码变为码词.

首先,在 $\mathbf{Z}_2[x]$ 内任意选定一个 $n-k$ 次多项式作为生成多项式. 下式为 $p(x)$ 除 $x^{n-k}m(x)$(n 次多项式)的带余除式:

$$x^{n-k}m(x) = q(x)p(x) + r(x)(r(x) = 0 \text{ 或 } \partial(r) < \partial(p)).$$

我们取 $w(x) = r(x) + x^{n-k}m(x)$ 为码词多项式.由于 $\mathbf{Z}_2[x]$ 中没有正负之分,



$$w(x) = r(x) - x^{n-k}m(x) = q(x)p(x),$$

从而 $p(x) \mid w(x)$.于是,接收者可以通过检验 $p(x) \mid w(x)$ 是否成立来判断码词是否正确.

例 1 以下我们以表格的形式说明如何设计一种(7,3) - 检错码:

$n - k$	4
$p(x)$	$1 + x^2 + x^3 + x^4$
信息码	101
信息码多项式 $m(x)$	$1 + x^2$
余式 $r(x)$	$1 + x$
码词多项式 $w(x)$	$r(x) + x^{n-k}m(x) = 1 + x + x^4 + x^6$
码词	1100 101 检验数字 信息

例 2 写出由多项式 $p(x) = 1 + x^2 + x^3$ 生成的信息码长 $k = 3$ 的一切码词.

解 由于 $\partial(p) = 3 = n - 3$,故码词的长 $n = 6$,信息码的个数为 $2^3 = 8$.按例 1 的方法我们可以得到下表:

	码词	
信息码	检验数字	信息码
000	000	000
100	101	100
010	111	010
001	110	001
110	010	110
101	011	101
011	001	011
111	100	111

最后我们指出,在实际当中在两端进行的多项式运算当然不是手工做的,都是由根据 $p(x)$ 和(n,k) - 码要求特殊设计的线路来完成的.即编码时,输入人员只需输入信息码,线路会将其转换成码词.接收时,也由线路来检验码词是否有错,并进行必要的纠码.本节仅显示了多项式编码的最基本的原理,到此为止,感兴趣的读者可参阅有关编码理论的专著.

习题 7－2

1.若生成多项式 $p(x) = 1 + x^2 + x^3 + x^4$,下面哪个码词有错:

(1)1011011;　　(2)1100101.

2.写出 $p(x) = 1 + x + x^3$ 生成的所有(6,3)－码.

7.3　尺规作图

1　尺规作图问题

在中学平面几何中,我们用直尺(没有刻度)和圆规可以作已知线段的垂直平分线,已知直线外一点作此直线的平行线,分定长的线段 n 等份,作已知角的平分线(将已知角二等分).以下是古希腊数学中的三大几何作图难题:

(1) 三等分角问题;

(2) 立方倍积问题,即作一个立方体使它的体积为一个已知立方体体积的两倍;

(3) 化圆为方问题,即作一个正方形使它的面积为一个已知半径之圆的面积.

这些问题在平面几何的范畴内是难以解决的,但利用近世代数的方法,这些问题可以较容易地得到解答.当然,近世代数的解决方法有时也依赖于其它领域的成果,如化圆为方问题最终是因为 π 是超越数而得到否定回答.在本节中,我们用近世代数语言简单讨论尺规作图的必要条件(限于篇幅我们不讨论充分条件,尽管对此也有确定的回答).由此我们可以回答上述的三个问题.在此,我们再一次看到了抽象知识的威力.

2　尺规作图的代数提法

建立平面直角坐标系,取定点(0,1)(确定单位长度).因为直线和圆都是由个别点决定的,因而尺规作图的已知条件本质上就是给定有限的几个点:

$$(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m) \qquad (T),$$

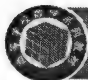
再在尺规所能的操作下连续不断地画出一些新的点,这些新的点称(T) **可构造点**,其坐标称(T) **可构造数**,即一个点是否(T)可构造等同于它的坐标是否为(T)可构造数.若(T)仅有点(0,1),则我们简称(T)可构造数为**可构造实数**.

尺规仅有如下两个操作:

(1) 通过已知或已作出的两点画直线;

(2) 以已知或已作出某个点(两个数)为心,以已知或已作出的某两个点之间的距离为半径画圆.

这两个操作产生新点的方式如下:



(1) 两条直线的交点 —— 新点.

每条已知或已作出的直线由四个已知的数决定,在坐标系内,其方程的系数由这四个数通过四则运算得到. 而求两条直线的交点就是解一个二元线性方程组,而其解可由方程组的系数通过四则运算得到.总之,新点的坐标可通过已知或已构造点坐标的四则运算得到.

(2) 直线与已有圆的交点 —— 新点.

求此交点的坐标就是解一个二元一次方程与一个二元二次方程(没有交叉项,且二次项的系数都为联立的方程组. 由于解此方程组,除了系数的四则运算外,最多会用到一个数(系数或系数的四则运算结果) 的平方根,因而新点的坐标可由已知点或已构造点的坐标通过四则运算和一个可构造数的平方根得到.

(3) 两圆的交点 —— 新点.

此时,我们可以得到与(2) 同样的结论.

总之,若造有理数域 $\mathbf{Q}$ 的扩域 $F_0 = \mathbf{Q}(x_1, y_1, \cdots, x_m, y_m)$,则第一个$(T)$ 可构造点的坐标在域 $F_1 = F_0$ 内或者在域 $F_1 = F_0(\sqrt{a})(a \in F_0)$ 内. 无论如何,都有$[F_1 : F_0] = 1$ 或2. 同理,第二个可构造点的坐标 F_1 在的扩域 F_2 内,且$[F_2 : F_1] = 1$ 或2.这样连续下去, 我们就得到了(T) 可构造数的必要条件.

定理 若实数 α 是(T) 可构造实数,则存在 F_0 的扩域 F 使得$\alpha \in F$,且$[F : F_0] = 2^k$ $(k \geqslant 0)$. 特别是, 若实数 α 是可构实数,则$[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^l(l \geqslant 0)$.

推论 60° 的角不能用尺规三等分.

证明 若能,如图 7 - 3,取此角的顶点为原点,点(0,1) 在其一边上,则我们就能构造一个直角三角形,其中一个角为 20°,取其斜边为 1, 因而可得到长为 cos20° 的线段(一个直角边), 即 cos20° 为可构造实数,从而

$$[\mathbf{Q}(\cos\alpha) : \mathbf{Q}]$$

应为 2 的幂.

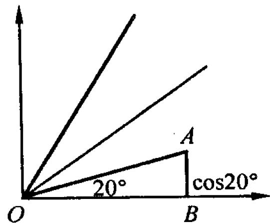


图 7 - 3

另一方面,在三角公式

$$\cos3\alpha = 4\cos^3\alpha - 3\cos\alpha$$

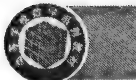
中代入 $\alpha = 20°$, 我们得知 cos20° 是方程 $\frac{1}{2} = 4x^3 - 3x$, 即 $8x^3 - 6x - 1 = 0$ 的解.但是,多项式 $8x^3 - 6x - 1$ 在 $\mathbf{Q}[x]$ 内不可约说明$[\mathbf{Q}(\cos\alpha) : \mathbf{Q}] = 3$. 这一矛盾证实了我们的结论.

评注:在这里我们仅由可构造数的必要条件证明了 60° 的角不能用尺规三等分,但这不是说任何一个角都不能尺规三等分.关于此问题,读者可阅读文献 2 的 216 ~ 224 页.

习题 7－3

1. 证明立方倍积问题的回答也是否定的.

2. 以 π 是超越数(即不是整系数多项式的根)为条件,证明化圆为方问题的回答也是否定的.



习题解答

说明:有些题的答案和解法不唯一,特别是证明题的方法很多,这里给出的答案仅供参考.

习题 1-1

2.首先,将一切正有理数排列如下(有重复),然后去掉重复,加上0,再一正一负排列,即得到与**Z**的一一对应:

$$1;$$
$$\frac{1}{2},\frac{2}{1};$$
$$\frac{1}{3},\frac{2}{2},\frac{3}{1};$$
$$\frac{1}{4},\frac{2}{3},\frac{3}{2},\frac{4}{1};$$
$$\frac{1}{5},\frac{2}{4},\frac{3}{3},\frac{4}{2},\frac{5}{1};$$
$$\cdots$$

3.$f: x\longmapsto \frac{1}{1-x}-\frac{1}{x}(0<x<1)$.

5.A 有 $1+C_n^1+C_n^2+\cdots+C_n^{n-1}+C_n^n=(1+1)^n$ 个不同的子集.

习题 1-2

2.$U_6=\{1,\varepsilon,\varepsilon^2,\cdots,\varepsilon^5\},\varepsilon=\cos\frac{2\pi}{6}+\mathrm{i}\sin\frac{2\pi}{6}$.

习题 1-3

3.如空间中向量的向量积,作为运算律下列两个等式不成立:

$\vec{a}\times\vec{b}=\vec{b}\times\vec{a}$, $(\vec{a}\times\vec{b})\times\vec{c}=\vec{a}\times(\vec{b}\times\vec{c})$.

4.分别用左分配律和右分配律展开 $(a_1\oplus a_2)\otimes(b_1\oplus b_2)$.

习题 1-4

1.(1) 是; (2) 不是; (3) 是; (4) 不是.

2.同构为 A 的恒同映射:$1_A : a \mapsto a$.

3.若 $\sigma : A \to B$ 为 A 到 B 的满同态,$\delta : B \to C$ 为 B 到 C 的满同态,则 $\delta\sigma$ 为 A 到 C 的满同态.

4.$\sigma : 1 \mapsto a, \varepsilon_1 \mapsto b, \varepsilon_2 \mapsto c$ 为 A 到 $(U_3, \cdot)$ 的同构.

5.$\sigma : a \mapsto -a$ 是 $(\mathbf{Q}, +)$ 的一个非恒同自同构.

6.$(a,b) \oplus (c,d) = (a+c, b+d)$,

$(a,b) \otimes (c,d) = (ac-bd, ad+bc)$.

7.反证.设 σ 为 $(\mathbf{Q}, +)$ 到 $(\mathbf{Q}^*, \cdot)$ 的同构,则存在有理数 a 使得 $\sigma(a) = 2$,从而得到不可能的等式

$$\left(\sigma\left(\frac{a}{2}\right)\right)^2 = \sigma\left(\frac{a}{2} + \frac{a}{2}\right) = \sigma(a) = 2.$$

习题 1 – 5

2.当 $a \neq b$ 时,$\bar{a} = \bar{b}$ 可能成立.如在 $\mathbf{Z}$ 中,$0 \neq 2$,但

$$\bar{0} = \bar{2} = \{0, \pm 2, \pm 4, \cdots\}.$$

3.是等价关系.$\mathbf{R}^* / \sim = \{\bar{1}, \overline{-1}\}$.

5.在 $(\mathbf{Z}_4, \circ)$ 中,当 $\bar{a} \neq \bar{0}, \bar{b} \neq \bar{0}$ 时,但可能出现 $\bar{a} \circ \bar{b} = \bar{0}$;在 $(\mathbf{Z}_5, \circ)$ 中,当 $\bar{a} \neq \bar{0}, \bar{b} \neq \bar{0}$ 时,$\bar{a} \circ \bar{b} \neq \bar{0}$.

7.有 $1 + \min\{m, n\}$ 个等价类.如 $M_{2\times3}(\mathbf{R})$ 有三个等价类,其典范代表元为 $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ 和 $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$,即任何一个 2×3 实矩阵都等价于其中之一.

习题 2 – 1

1.反证.若 T_A 中的元 $\sigma : 1 \mapsto 2, 2 \mapsto 2$ 有逆元 $\delta \in T_A$,则 $\sigma\delta = 1_A$,从而推得矛盾 $2 = \delta(\theta(1)) = 1_A(1) = 1$.

2.$a^2 = e \Rightarrow a = a^{-1}$;$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

3.注意:

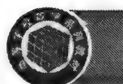
$o(a) = o(a^{-1})$;$o(e) = 1$;$a^2 = e \Leftrightarrow a = a^{-1}$;$o(a) > 2 \Leftrightarrow a \neq a^{-1}$.

4.用上题的结论.

5.反证.若 a 的阶无限,则 $a, a^2, a^3, \cdots$ 互不相同.

7.$(\Rightarrow)$ $o(a) = n \Rightarrow a^n = e$;若 $a^m = e(m \geqslant 1)$,令 $m = qn + r, 0 \leqslant r < n$,则 $e = a^m = a^{qn}a^r = (a^n)^q a^r = a^r \Rightarrow r = 0 \Rightarrow n \mid m$;

$(\Leftarrow)$ n 就是使 $a^n = e$ 的最小正整数.



8.$(0,\bar{0})$ 是零元;群是无限群;$(0,\bar{1})$ 的阶为 2,但不是零元;$(1,\bar{0})$ 的阶无限.

9.$(\Rightarrow)$ $x = a^{-1}b, y = ba^{-1}$ 是方程 $ax = b, ya = b$ 的解.

$(\Leftarrow)$ 由定理 2,只须证明 G 满足(A)和(B):

(A) 任取 $b \in G$.对于方程 $yb = b$,由(C)知,存在 $e \in G$ 使 $eb = b$.现在任取 $a \in G$.对于方程 $bx = a$,由(C)知,存在 $c \in G$ 使 $bc = a$.于是,$ea = e(bc) = (eb)c = bc = a$.

(B) 对于方程 $ya = e$,由(C)知存在 $a^{-1} \in G$ 使 $a^{-1}a = e$.

10.证明半群 G 满足条件(C).设 $G = \{a_1, \cdots a_n\}$, $a, b \in G$. 由于左消去律成立,故 $G = \{aa_1, \cdots, aa_n\}$.从而,存在某个 a_i 使 $aa_i = b$,即方程 $ax = b$,在 G 有解.同样,由右消去律可以说明方程 $xa = b$ 在 G 有解成立.

习题 2-2

1.不一定.例如,$\sigma: n \mapsto \bar{n}$ 为$(\mathbf{Z}, +)$到$(\mathbf{Z}_2, +)$的同态,1 在$(\mathbf{Z}, +)$中的阶无限,但 $\sigma(1) = \bar{1}$ 在$(\mathbf{Z}_2, +)$中的阶为 2.

2.是的.$\sigma: \bar{n} \mapsto \bar{n}$ 为同态.

3.是的.$\sigma: n \mapsto \bar{n}$ 为同态.

4.不是交换群.单位元为 $l_{1,0}$, $l_{a,b}^{-1} = l_{a^{-1}, -a^{-1}b}$, $l_{a,b}l_{c,d} = l_{ac, ad+b}$;不是交换群,例如,$l_{1,2}l_{2,1} = l_{2,3}$, $l_{2,1}l_{1,2} = l_{2,5}$.

5.是交换群.

6.

	I	R	R^2	T_1	T_2	T_3
I	I	R	R^2	T_1	T_2	T_3
R	R	R^2	I	T_3	T_1	T_2
R^2	R^2	I	R	T_2	T_3	T_1
T_1	T_1	T_2	T_3	I	R	R^2
T_2	T_2	T_3	T_1	R^2	I	R
T_3	T_3	T_1	T_2	R	R^2	I

习题 2-3

1.$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$,

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$;

	(1)	(123)	(132)	(23)	(12)	(13)
(1)	(1)	(123)	(132)	(23)	(12)	(13)
(123)	(123)	(132)	(1)	(12)	(13)	(23)
(132)	(132)	(1)	(123)	(13)	(23)	(12)
(23)	(23)	(13)	(12)	(1)	(132)	(123)
(12)	(12)	(23)	(13)	(123)	(1)	(132)
(13)	(13)	(12)	(23)	(132)	(123)	(1)

2. S_3 中与(123)交换的元为(1),(123),(132).

3. 直接验证.

4. 说明 k 次幂为(1),小于 k 次的幂不是(1).

5. 利用$(1i)(1j)(1i) = (ij)$.

习题 2-4

2. $(r,n) = 1 \Rightarrow pr + qn = 1 \Rightarrow a^k = a^{k(pr+qn)} = (a^r)^{kp}$.

3. 由习题2-1-6,要证明$(a^r)^{\frac{n}{d}} = e$,且当$(a^r)^m = e$时,$\frac{n}{d} \mid m$.

令 $n = dk, r = dl$,则$(k,l) = 1$,$(a^r)^{\frac{n}{d}} = a^{\frac{rn}{d}} = a^{nl} = e$;

$(a^r)^m = e \Rightarrow a^{rm} = e \Rightarrow n \mid rm \Rightarrow k \mid lm \Rightarrow k \mid m\left(k = \frac{n}{d}\right)$.

4. 设 $\sigma: G \to \bar{G}$ 为同态,且 $G = (a)$,证明 $\bar{G} = (\sigma(a))$.

5. 设 $G = (a)$,$\bar{G} = (\bar{a})$,证明 $\sigma: a^k \mapsto \bar{a}^{-k}$ 为 G 到 $\bar{G}$ 的满同态.

6. $D_3 = \{(1),(23),(13),(12),(123),(132)\}$,$D_3 \cong S_3$ 明显.

7.

	e	r	r^2	r^3	t	rt	r^2t	r^3t
e	e	r	r^2	r^3	t	rt	r^2t	r^3t
r	r	r^2	r^3	e	rt	r^2t	r^3t	t
r^2	r^2	r^3	e	r	r^2t	r^3t	t	rt
r^3	r^3	e	r	r^2	r^3t	t	rt	r^2t
t	t	r^3t	r^2t	rt	e	r^3	r^2	r
rt	rt	t	r^3t	r^2t	r	e	r^3	r^2
r^2t	r^2t	rt	t	r^3t	r^2	r	e	r^3
r^3t	r^3t	r^2t	rt	t	r^3	r^2	r	e



习题 2－5

1. $\{(1)\}$, $\{(1),(12)\}$, $\{(1),(23)\}$, $\{(1),(13)\}$, $\{(1),(123),(132)\}$, S_3.

2. 直接验证.

3. 由于 $\{(1),(123),(132)\} \cup \{(12)\} \subset (S)$, S_3 没有 4 阶和 5 阶子群,故 $(S) = S_3$.一个群的两个不同的集会生成相同的子群,例如,$((123)) = ((132)) = \{(1),(123),(132)\}$.

5. 设 $H < G = (a)$. 由于 $a^k \in H \Leftrightarrow (a^k)^{-1} = a^{-k} \in H$,故使 $a^m \in H$ 的最小正整数 m 存在.事实上,$H = (a^m)$,这是因为

$$
\begin{aligned}
a^k \in H, k = qm + r(0 \leqslant r < m) &\Rightarrow a^k = a^{qm+r} = a^{qm}a^r \\
&\Rightarrow a^r = a^k(a^m)^{-q} \in H \\
&\Rightarrow r = 0 \\
&\Rightarrow a^k = (a^m)^q.
\end{aligned}
$$

7. 证明群中非单位元的阶是这个素数(群的阶).

8. 任取此群的非单位元 a,则 $o(a) \mid p^m$,从而 $o(a) = p^k(0 < k \leqslant m)$. 于是,$o(a^{p^{k-1}}) = p$,子群 $(a^{p^{k-1}})$ 的阶为 p.

9. 设 $o(a) = k, o(b) = l$,则 $(ab)^{kl} = e$.再由下面的推理知命题成立:

$$
\begin{aligned}
(ab)^m = e &\Rightarrow a^m b^m = e \Rightarrow a^m = (b^{-1})^m \\
&\Rightarrow a^{km} = (b^{-1})^{km} = e, a^{lm} = (b^{-1})^{lm} = e \\
&\Rightarrow k \mid lm, l \mid km \Rightarrow k \mid m, l \mid m \Rightarrow kl \mid m.
\end{aligned}
$$

11. 设群 G 的阶为 4. 若 G 中有一个元的阶为 4,则 G 为循环群.若 G 中没有阶为 4 的元,则 $G = \{e,a,b,c\}$ 中的元除单位元 e 外,阶都是 2,此时 G 为交换群,$ab = c, bc = a, ca = b$.此群明显是同构于 Klein 四元群.

12. $(\Rightarrow)$ 子群的定义.

$(\Leftarrow)$ H 中结合律自然成立,再加之运算封闭,故 H 是半群.又两个消去律在 H 中也自然成立,由习题 2－1－7 知 $H < G$.

13. (1) 例行公事可验证 $\sim$ 为 $H \times K$ 上的等价关系.

(2) (h,k) 代表的等价类 $\overline{(h,k)} = \{(x,y) \mid xy = hk\}$,即 $H \times K$ 有 $|HK|$ 个等价类.又

$$
\begin{aligned}
(x,y) \in \overline{(h,k)} &\Leftrightarrow xy = hk \Leftrightarrow yk^{-1} = x^{-1}h = a \in H \cap K \\
&\Leftrightarrow x = ha^{-1}, y = ak(a \in H \cap K)
\end{aligned}
$$

说明每个等价类中包含 $|H \cap K|$ 个 (h,k).总之,等式成立.

习题 2－6

1. $N = \{e,n\}, g^{-1}ng \in N, n \neq e \Rightarrow g^{-1}ng = n \Rightarrow ng = gn \Rightarrow n \in Z(G)$.

2. 由定义直接验证.

3. $a \notin N \Leftrightarrow aN \neq N \Leftrightarrow aN \cap N = \varnothing$;

$a \notin N \Leftrightarrow Na \neq N \Leftrightarrow Na \cap N = \varnothing$;

$[G:N] = 2 \Rightarrow G = aN \cup N = Na \cup N (a \notin N)$

$\Rightarrow aN = Na$.

4. 令 $a = h_1 n_1, b = h_2 n_2$. 由下面的推理知 $HN < G$:

$$ab = h_1 n_1 h_2 n_2 = (h_1 h_2)[(h_2^{-1} n_1 h_2) n_2] \in HN,$$

$$a^{-1} = (h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = nh = h(h^{-1} nh) \in HN.$$

5. (1) 例行公事, 可验证 C 是 G 的子群. 再注意

$$\begin{aligned} g^{-1}[a,b]g &= g^{-1}a^{-1}b^{-1}abg = (g^{-1}a^{-1})b^{-1}abg \\ &= [(ag)^{-1}b^{-1}(ag)b][b^{-1}g^{-1}bg] \\ &= [ag,b][b,g] \in C; \end{aligned}$$

$g^{-1}[a,b][c,d]g = (g^{-1}[a,b]g)(g^{-1}[c,d]g) \in C$.

(2) $aC \cdot bC = bC \cdot aC \Leftrightarrow abC = baC = baC$

$\Leftrightarrow (ba)^{-1}(ab) = [a,b] \in C$.

(3) 我们只要说明每个换位子 $[a,b] \in N$:

$$aN \cdot bN = bN \cdot aN \Leftrightarrow abN = baN$$

$$\Leftrightarrow (ba)^{-1}(ab) = [a,b] \in N \Rightarrow C \subset N.$$

习题 2－7

3. 证明 $\bar{\sigma}: g \mapsto \sigma(g)N'$ 是群 G 到 G'/N' 的满同态, 再证明 $\ker\bar{\sigma} = N$ 即可.

4. $(\Rightarrow)\sigma: G \to G'$ 为满同态, 则 $G/\ker\sigma \cong G'$. 从而

$$|G| = |\ker\sigma| \cdot |G'|.$$

$(\Leftarrow)$ 设 $G = (a), (o)a = n; G' = (b), (o)b = m, m \mid n$. 令

$$\sigma: a^k \mapsto b^k.$$

只要 σ 是映射, 其保持运算是明显的. 推理:

$$a^k = a^l \Leftrightarrow n \mid (k-l) \Rightarrow m \mid (k-l) \Rightarrow b^k = b^l$$

说明了 σ 是映射.

5. $G = (a), N < G \Rightarrow G/N = (aN)$.

习题 2－8

1. 作为集合, 直接证明两边互相包含.

2. 轨道就一个 S_L, $\mathrm{stab}\,aH = aHa^{-1}$.

3. 利用有限群的类方程证明 p 整除 $|C|$.



习题 3－1

1.令 $ab=0$.

2.$(ma)(na)=(na)(ma)=(mn)a^2$.

3.只需验证加法和乘法是封闭的.

4.用左分配律和右分配律展开 $2(a+b)$:

$$2(a+b)=2a+2b=a+a+b+b,$$
$$\begin{aligned}2(a+b)&=(1+1)(a+b)=(a+b)+(a+b)\\&=a+b+a+b\\&\Rightarrow a+a+b+b=a+b+a+b\\&\Rightarrow a+b=b+a\end{aligned}$$

5.$(k,n)=1\Rightarrow pk+qn=1\Rightarrow \bar{p}\bar{k}=1$.

6.令 $a^m=0,a^n=0$ 则

$$\begin{aligned}(a+b)^{m+n}&=a^{m+n}+C_{m+n}^{1}a^{m+n-1}b+\cdots+C_{m+n}^{n-1}a^{m+1}b^{n-1}\\&\quad+C_{m+n}^{n}a^{m}b^{n}+C_{m+n}^{n+1}a^{m-1}b^{n+1}+\cdots+b^{m+n}\\&=0+\cdots+0=0.\end{aligned}$$

在 $\mathbf{Z}_4$ 中 $\bar{2}\neq 0,\bar{2}\cdot\bar{2}=0$.

7.(1)⇒(2):自然;

(2)⇒(1):

$$a^m=0\Rightarrow a^{2^k}=0\Rightarrow a^{2^{k-1}}=0\Rightarrow\cdots\Rightarrow a^2=0\Rightarrow a=0$$

8.首先,$(a+b)^2=a+b\Rightarrow ab+ba=0\Rightarrow ab=-ba$.令 $a=b$ 得到 $2a^2=2a=0$.从而 $a=-a,ab=-ba=ba$.

9.令 $(1-ab)^{-1}=c$,即 $c(1-ab)=(1-ab)c=1$.我们有

$$\begin{aligned}c(1-ab)=1&\Rightarrow c-cab=1\Rightarrow ca=caba=a\Rightarrow ca(1-ba)=a\Rightarrow bca(1-ba)=ba\\&\Rightarrow -bca(1-ba)=-ba\Rightarrow 1-bca(1-ba)=1-ba\\&\Rightarrow (1-ba)+bca(1-ba)=1\Rightarrow (1-ba)(1+bca)=1.\end{aligned}$$

同理 $(1-ab)c=1\Rightarrow(1+bca)(1-ba)=1$.总之,

$$(1-ba)^{-1}=1+bca.$$

习题 3－2

1.(1)4 的素因子只有 2;

(2) 令 $F^*=\{1,a,b\}$,则 $a+1=b,b+1=a$.因 $|F^*|=3$,故

$$a^2=b=a+1,\quad b^2=a=b+1.$$

4.首先,$(a,n)=1\Rightarrow pa+qn=1$.因而

$$
\begin{aligned}
b\in\bar{a} &\Rightarrow n\mid(b-a)\Rightarrow b-a=kn\Rightarrow b=a+kn\\
&\Rightarrow pb=pa+pkn=1-qn+pkn\\
&\Rightarrow pb+(q-pk)n=1\\
&\Rightarrow(b,n)=1.
\end{aligned}
$$

5.只要证明$(a,n)=1,(b,n)=1\Rightarrow(ab,n)=1$,这是明显的.

6.由上题,$(a,n)=1\Rightarrow\bar{a}^{\phi(n)}=\bar{1}\Rightarrow n\mid(a^{\phi(n)}-1)\Rightarrow a^{\phi(n)}\equiv1(\mathrm{mod}\,n)$.

习题 3－3

3.设 F 为特征 0 的域,e 为其单位元.令

$$Q=\{(pe)(qe)^{-1}\mid p,q\in\mathbf{Z},q\neq0\}$$

则 $\sigma:\frac{p}{q}\longmapsto(pe)(qe)^{-1}$ 为 $\mathbf{Q}$ 到 Q 的同构.

4.加群 $\mathbf{Z}_3$ 的一切自同构为:

$$\sigma:\bar{0}\longmapsto\bar{0},\bar{1}\longmapsto\bar{1},\bar{2}\longmapsto\bar{2};\quad\delta:\bar{0}\longmapsto\bar{0},\bar{1}\longmapsto\bar{2},\bar{2}\longmapsto\bar{1};$$

域 $\mathbf{Z}_3$ 的一切自同构仅有上述的恒同映射 σ 一个.

5.由于 $\mathrm{i}^2=-1$,若 σ 为自同构,则$(\sigma(\mathrm{i}))^2=-\sigma(1)=-1$,即

$$\sigma(\mathrm{i})=\mathrm{i}\text{ 或 }\sigma(\mathrm{i})=-\mathrm{i};$$

另一方面,$\mathbf{Q}(\mathrm{i})$ 确实有两个满足上述条件的自同构.

习题 3－4

1.证明 $R[x]$ 无零因子,即 $f(x)\neq0,g(x)\neq0\Rightarrow f(x)g(x)\neq0$. 由于 R 是整环,无零因子,这一点正确:

$$
\left.\begin{aligned}
f(x)\neq0\Rightarrow f(x)=a_nx^n+\cdots+a_0\neq0,a_n\neq0\\
g(x)\neq0\Rightarrow g(x)=b_mx^m+\cdots+b_0\neq0,b_m\neq0
\end{aligned}\right\}\Rightarrow a_nb_m\neq0
$$

$$\Rightarrow f(x)g(x)=a_nb_mx^{m+n}+\cdots+a_0b_0\neq0.$$

3.$x^{p^2}-x^p+1=(x^p-x+1)^p$.

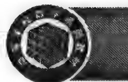
习题 3－5

1.直接验证得 $I=\{4r\mid r\in R\}$ 是 R 的理想.但

$$4=4\times0+4\times1\in(4)=\{4r+4n\mid r\in R,n\in\mathbf{Z}\},$$

而 $4\notin I=\{8n\mid n\in\mathbf{Z}\}$.

2.说明 $1\in(3,7)$.



3. $1=\frac{1}{2}\cdot 2+0\cdot x\in(2,x)\Rightarrow(2,x)=(1)=\mathbf{Q}[x]$

5. $\{0\},\{0,\bar{3}\},\{0,\bar{2},\bar{4}\},\mathbf{Z}_6$

6. 首先，

$$a+bi=a+bi+b-b=(a-b)+b(1+i)$$
$$\Rightarrow(a+bi)+I=(a-b)+I$$

说明 $R/(1+i)=\{n+I|\{n\in\mathbf{Z}\}$；另一方面，

$$\begin{aligned}n+I=m+I&\Leftrightarrow n-m\in I\\&\Leftrightarrow n-m=(a+bi)(1+i)\\&\Leftrightarrow n-m=a-b,0=a+b\\&\Leftrightarrow n-m=2a\end{aligned}$$

说明 $2k+I=I,(2k+1)+I=1+I$. 总之，

$$R/(1+i)=\{I,1+I\}.$$

7. 在 $\mathbf{Z}[x]$ 中，$(2,x)$ 是常数项为偶数的一切多项式.假设 $(2,x)=(p(x))$ 为主理想，则 $2=q(x)p(x),x=r(x)p(x)$. 前者说明 $p(x)=\pm 1,\pm 2$. 若 $p(x)=\pm 1$，则 $(2,x)=(p(x))=\mathbf{Z}[x]$，这不可能. 若 $p(x)=\pm 2$，这也同 $x=r(x)p(x)$ 矛盾.

习题 3 - 6

1. 由习题 3 - 5 - 6 知 $R/(1+i)$ 有两个元，零元和单位元，从而为域.

2. (x) 不是 $\mathbf{Z}[x]$ 的极大理想，因为 $\mathbf{Z}[x]$ 为有单位元的交换环，但 $\mathbf{Z}[x]/(x)\cong\mathbf{Z}$ 不是域. 同理 (x) 是 $\mathbf{Q}[x]$ 的极大理想.

3. 当时 $a\neq 0,(a)=R$，从而 a 可逆.

4. 首先，注意，在环 $2\mathbf{Z}$ 中，$(4)=\{4r+4n|r\in 2\mathbf{Z},n\in\mathbf{Z}\}=\{4(2m+n)|m,n\in\mathbf{Z}\}$.

若 $(4)\subset I\lhd\mathbf{Z},(4)\neq I$，则存在 $2k\in I,2k\notin(4)$. 而

$$2k\notin(4)=\{4(2m+n)|m,n\in\mathbf{Z}\}\Rightarrow k\notin\{4m+2n|m,n\in\mathbf{Z}\}$$

说明 $k=4q+1$ 或 $k=4q+3$. 前者说明

$$2=2k-(2q)\cdot 4\in I\Rightarrow I=2\mathbf{Z};$$

后者说明

$$2=2k-(2q+1)\cdot 4\in I\Rightarrow I=2\mathbf{Z}.$$

$2\mathbf{Z}/(4)$ 没有单位元，从而不是域.

5. $(m,n)=1\Rightarrow pm+qn=1(p,q\in\mathbf{Z})$. 在 R 的商域 Q 内，

$$a=a^{pm+qn}=(a^m)^p+(a^n)^q+(b^m)^p+(b^n)^q=b^{pm+qn}=b.$$

6. $Z_2[x]/I=\{I,1+I,x+I,(1+X)+I\}$.

习题 4－1

1.(1) 在 $\mathbf{Q}[x]$，$q(x)=\frac{1}{3}x-\frac{7}{9}$，$r(x)=-\frac{26}{9}x-\frac{2}{9}$；

在 $\mathbf{Z}_5[x]$，$q(x)=2x+2$，$r(x)=x-3$；

(2) 在 $\mathbf{Q}[x]$，$q(x)=x^2+x-1$，$r(x)=-5x+6$；

在 $\mathbf{Z}_5[x]$，$q(x)=x^2+x-1$，$r(x)=1$.

2.(1) 在 $\mathbf{Q}[x]$，$(f(x),g(x))=x+1$；

在 $\mathbf{Z}_5[x]$，$(f(x),g(x))=1$；

(2) 在 $\mathbf{Q}[x]$，$(f(x),g(x))=1$；

在 $\mathbf{Z}_5[x]$，$(f(x),g(x))=1$.

3.$f_1\mid g\Rightarrow g=h_1f_1$，$f_2\mid g\Rightarrow g=h_2f_2$；

$(f_1,f_2)=1\Rightarrow pf_1+qf_2=1\Rightarrow gpf_1+gqf_2=g\Rightarrow ph_2f_1f_2+h_1qf_1f_2=g\Rightarrow f_1f_2\mid g$.

习题 4－2

1.$x^3+x^2+x+1=(x+1)^3$.

2.$x^3-1=(x-1)^3$.

3.反证.由于 $x^4+x^3+x^2+x+1$ 在 $\mathbf{Z}_2$ 内无根，故若在 $\mathbf{Z}_2[x]$ 内可约，其为两个二次不可约多项式的乘积，而 $\mathbf{Z}_2[x]$ 的二次不可约多项式仅有 x^2+x+1.于是，我们得到矛盾的等式：

$$x^4+x^3+x^2+x+1=(x^2+x+1)^2=x^4+x^2+1.$$

习题 4－3

1.$f(x)=(x^2+2)^2$.

2.由于 $F[x]\subset E[x]$，故在 $E[x]$ 内仍有 $(f(x),f'(x))=1$.从而，在域 E 内 $f(x)$ 仍然没有重根.

3.$x^5-x=x(x-1)(x-2)(x-3)(x-4)$.

习题 4－4

1.(1)2；(2)－1,3.

2.由于 $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1=\frac{x^p-1}{x-1}$，故

$$\Phi_p(x+1)=\frac{(x+1)^p-1}{x}=x^{p-1}+C_p^1x^{p-2}+\cdots+C_p^{p-2}x+p.$$

由 Eisenstein 定理，$\Phi_p(x+1)$ 在 $\mathbf{Q}[x]$ 内不可约，从而 $\Phi_p(x)$ 在 $\mathbf{Q}[x]$ 内不可约.



习题 5 - 1

2. $[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}]=[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2\times 2=4$;
$\mathbf{Q}(\sqrt{2},\sqrt{3})$ 在 $\mathbf{Q}$ 上的一个基可取为 $1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}$.

3. 作为 $\mathbf{Q}$ 上的线性空间,$\mathbf{Q}(\sqrt{2})$ 和 $\mathbf{Q}(\mathrm{i})$ 都是二维的,从而同构.但作为域它们不同构,若它们同构,$\mathbf{Q}(\mathrm{i})$ 到 $\mathbf{Q}(\sqrt{2})$ 的同构为 σ,则由 $\mathrm{i}^2=-1$,我们可得到$(\sigma(\mathrm{i}))^2=-\sigma(1)=-1$,但 $\mathbf{Q}(\sqrt{2})$ 中没有平方为 -1 的元.

习题 5 - 2

1. $\frac{2\mathrm{i}+1}{\mathrm{i}-1}=\frac{1}{2}-\frac{3}{2}\mathrm{i}$,$\frac{2\mathrm{i}+1}{\mathrm{i}-1}$ 在 $\mathbf{Q}[x]$ 上的极小多项式为

$$[x-(\frac{1}{2}-\frac{3}{2}\mathrm{i})][x-(\frac{1}{2}+\frac{3}{2}i)]=x^2-x+\frac{5}{2};$$

i 在 $\mathbf{Q}[x]$ 上极小多项式为 x^2+1. 由于这两个多项式不同,故 $\mathbf{Q}(\mathrm{i})$ 与 $\mathbf{Q}(\frac{2\mathrm{i}+1}{\mathrm{i}-1})$ 不同构.

2. $(u^2+u+1)(u^2-u)=-2u+2$,$(u-1)^{-1}=-\frac{1}{3}u^2-\frac{1}{3}$.

3. $\omega=\cos\frac{2\pi}{12}+\mathrm{i}\sin\frac{2\pi}{12}$ 是 $x^{12}-1=0$ 的根. $x^{12}-1=0$ 在 $\mathbf{Q}[x]$ 内的标准分解式为

$$\begin{aligned}x^{12}-1&=(x^6+1)(x^6-1)\\&=(x^2+1)(x^4-x^2+1)(x^3-1)(x^3+1)\\&=(x^2+1)(x^4-x^2+1)(x-1)(x^2+x+1)(x+1)(x^2-x+1)\\&=(x-1)(x+1)(x^2+1)(x^2-x+1)(x^2+x+1)(x^4-x+1).\end{aligned}$$

x^4-x^2+1 是 ω 在 $\mathbf{Q}$ 上的极小多项式,$[\mathbf{Q}(\omega):\mathbf{Q}]=4$.

习题 5 - 3

1. 由条件,设 $e_0+e_1\alpha+\cdots+e_n\alpha^n=0,e_0,e_1,\cdots,e_n\in E$,则 α 是 $E_1=F(e_0,e_1,\cdots,e_n)$ 上的一个代数元,$E_1(\alpha)/F$ 为有限扩域.另一方面,由于 E/F 为代数扩域,故 $e_0,e_1,\cdots,e_n$ 是 F 上的一个代数元,E_1/F 是有限扩域,从而 $E_1(\alpha)/F$ 也是有限扩域.于是,α 是 F 上的一个代数元.

2. 令 $\alpha_1,\cdots\alpha_m$ 是 E 在 F 上的基,则 $E=F(\alpha_1,\cdots,\alpha_m)$.

3. 要证$[I(\alpha):I]=n$.设$[I(\alpha):I]=k$,则由

$$[I(\alpha):F]=[I(\alpha):I][I:F]=k\cdot m;$$
$$[I(\alpha):F]=[I(\alpha):F(\alpha)][F(\alpha):F]=l\cdot n,$$

我们得到 $n\mid km$,从而 $n\mid k$,$k\geqslant n$.另一方面,由于 $F\subset I$,故 α 在I上的极小多项式的次数不高

于它在 F 上的极小多项式的次数，即 $k \leqslant n$.于是 $k = n$.

4.($\Rightarrow$) 由于$[E:I]=2$,故 $\gamma \in E - I$ 在I 上的极小多项式为

$$x^2 + ix + j$$

即 $\gamma^2 + i\gamma + j = 0$.但,由于 F 的特征不是2,

$$\gamma^2 + i\gamma + j = 0 \Rightarrow \gamma^2 + 2\frac{i}{2}\gamma + \frac{i^2}{4} + (j - \frac{i^2}{4}) = 0$$

$$\Rightarrow (\gamma + \frac{i}{2})^2 + (j - \frac{i^2}{4}) = 0$$

故 E 内存在元素α,其在 I 上的极小多项式为$x^2 + i$.同理,I 内存在元素β,其在 F 上的极小多项式为 $x^2 + f$.设 $i = a\beta + b, a, b \in F$,则

$$\alpha^2 + i = 0 \Rightarrow \alpha^4 = i^2 = a^2\beta^2 + 2ab\beta + b^2 = -a^2f + 2b(-\alpha^2 - b) + b^2$$

$$= -2b\alpha^2 - b^2 - a^2f \Rightarrow \alpha^4 + (2b)\alpha^2 + (b^2 + a^2f) = 0.$$

从而$E = F(\alpha)$,且 α 在F 上的极小多项式为$x^4 + ax^2 + b$.($\Leftarrow$)$I = F(\alpha^2)$ 满足要求.

习题 5 - 4

1.取 $\alpha = \cos\frac{2\pi}{8} + \mathrm{i}\sin\frac{2\pi}{8}$,则 $\alpha, \alpha^3, \alpha^5, \alpha^7$ 是 $x^4 + 1$ 的一切根,它们都含在 $\mathbf{Q}(\alpha)$.于是,$x^4 + 1$ 在 $\mathbf{Q}$ 上的分裂域是单扩域 $\mathbf{Q}(\alpha)$,其中 $\alpha^4 + 1 = 0$.

2.由分裂域的唯一性,我们不妨假设.$\beta \in \mathbf{C}$.令 $\varepsilon = e^{\frac{2\pi}{3}\mathrm{i}}$,则

$$x^3 - a = x^3 - \beta^3 = (x - \beta)(x - \beta\varepsilon)(x - \beta\varepsilon^2).$$

于是,$x^3 - a$ 在 $\mathbf{Q}$ 上的分裂域为 $\mathbf{Q}(\beta, \beta\varepsilon, \beta\varepsilon^2) = \mathbf{Q}(\beta)(\varepsilon)$.由于,$\varepsilon \notin \mathbf{Q}(\beta)$ 故 $\mathbf{Q}(\beta)$ 不是 $x^3 - a$ 在 $\mathbf{Q}$ 上的分裂域.

3.令 E/F 为$p_1(x)\cdots p_m(x)$的分裂域.在E/F 中取$\alpha_1, \cdots, \alpha_m$ 使它们分别为$p_1(x), \cdots, p_m(x)$的根,则 $E = F(\alpha_1, \cdots, \alpha_m)$ 满足要求.

4.由 $x^p - a = x^p - \beta^p = (x - \beta)^p$ 知$F(\beta)/F$ 是$x^p - a$ 的分裂域.

5.(1) 由 $f'(x) = (x^p - x - a)' = px^{p-1} - 1 = -1$ 知 $f(x)$ 没有重根.

(2) 令 E/F 是$f(x)$ 的分裂域,$\beta \in E$ 是$f(x)$ 的一个根.由

$$f(\beta + 1) = (\beta + 1)^p - (\beta + 1) - a = \beta^p + 1 - \beta - 1 - a = f(\beta) = 0,$$

我们得到

$$f(x) = (x - \beta)[x - (\beta + 1)]\cdots[x - (\beta + p - 1)].$$

若 $f(x)$ 在 $F[x]$ 内可约,则 $f(x)$ 的上述分解式的 $k(0 < k < p)$ 个一次式之积为 $F[x]$ 中的多项式.由此乘积的次高项的系数可以推出$\beta \in F$,即$f(x)$在 F有根.反之,若$f(x)$在 F有根,则 $f(x)$ 在 $F[x]$ 内就可以分解为一次式的乘积,可约.

6.设 $f(x) = p_1(x)p_2(x)$ 有重根,则$(f(x), f'(x)) = d(x) \neq 1$. 由 $d(x) \mid p_1(x)p_2(x)$,



我们得到 $d(x)=p_1(x),d(x)=p_2(x)$ 或 $d(x)=p_1(x)p_2(x)$. 若 $d(x)=p_1(x)$,再由 $d(x)\mid f'(x)$,及

$$f'(x)=p_1'(x)p_2(x)+p_1(x)p_2'(x)$$

知 $p_1(x)\mid p_1'(x)p_2(x)$.从而

$p_1(x)\mid p_1'(x)\Rightarrow p_1'(x)=0\Rightarrow(p_1(x),p_1'(x))=p_1(x)\neq 1,p_1(x)$ 有重根,矛盾.

同样,$d(x)=p_2(x)$ 也不能成立.

若 $d(x)=p_1(x)p_2(x)$,则 $f(x)\mid f'(x)$,从而 $f'(x)=0$, 即

$$p_1'(x)p_2(x)=-p_1(x)p_2'(x).$$

由此,$p_2(x)\mid p_1(x)p_2'(x)$,这也不可能.

习题 5－5

1.$q=p^{km}$,我们断言$(x^{p^m}-x)\mid(x^q-x)$.这由下面的运算可以看出:

$$x^q-x=x(x^{p^{km}-1}-1)=x(x^{(p^m-1)(p^{m(k-1)}+p^{m(k-2)}+\cdots+1)}-1)$$
$$=x(x^{p^m-1}-1)k(x)=(x^{p^m}-x)k(x).$$

这说明 x^q-x 的分裂域 $\mathbf{F}_{(p^n)}$ 中包含 $x^{p^m}-x$ 的分裂域,一个有 p^m 个元的子域.另一方面,F 的有 p^m 个元的子域是 $x^{p^m}-x$ 的分裂域,而 x^q-x 没有重根,因而这样的子域唯一.

2.因为分裂域是代数扩域,由上题,这是明显的.

3.$x^p-x=x(x-1)(x-2)\cdots(x-(p-1))$.

4.x^3+x+1,x^3+x^2+1.

5.(1) 说明 x^3+x^2+1 在 $\mathbf{Z}_2[x]$ 内不可约;

(2)$\mathbf{Z}_2/I=\{I,1+I,x+I,(1+x)+I,x^2+I,(1+x^2)+I,(x+x^2)+I,(1+x+x^2)+I\}$;

(3) 由(2) 可知;

(4)$\mathbf{Z}_2[x]/(x^3+x+1)$ 也为域,且与 $\mathbf{Z}_2[x]/I$ 同构.

6.(1)$F=\mathbf{F}_g[x]/I$ 为域,有 q^n 个元素,$\mathbf{F}^*$ 为 q^n-1 元的乘法群,从而

$$(x+I)^{q^n-1}=1+I$$

即 $x^{q^n-1}\in I,p(x)\mid(x^{q^n-1}-1)$,进而

$$p(x)\mid(x^{q^n}-x)$$

(2) 由于$(x^{q^n}-x)'=-1$,从而 $x^{q^n}-x$ 没有重根;再由(1) 知 $p(x)$ 没有重根.

习题 6－1

1.(1) 不是;(2) 不是;(3) 是.

2. A 上满足条件的一切偏序关系为:

$\{(a,a),(b,b),(c,c),(a,b)\}$,

$\{(a,a),(b,b),(c,c),(a,b),(a,c)\}$,

$\{(a,a),(b,b),(c,c),(a,b),(c,b)\}$,

$\{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c)\}$,

$\{(a,a),(b,b),(c,c),(a,b),(c,b),(c,a)\}$,

$\{(a,a),(b,b),(c,c),(a,b),(c,b),(a,c)\}$.

3. 对比它们的哈氏图建立同构.

习题 6－2

1. 不是,$2 \wedge 3$ 不存在.

3. (1) 是;(2) 是;(3) 是;(4) 不是.

4. 证明 $x \leqslant y$ 及 $y \leqslant x$. 由对称性,只要证明一个:

$$
\begin{aligned}
y \leqslant y \vee (y \wedge a) &= (y \wedge y) \vee (y \wedge a) \\
&= y \wedge (y \vee a) \\
&= y \wedge (x \vee a) \\
&= (y \wedge a) \vee (y \wedge x) \\
&= (x \wedge a) \vee (y \wedge x) \\
&= x \wedge (y \vee a) \leqslant x.
\end{aligned}
$$

5. $x = x' \Rightarrow x = x \vee x = 1, x = x \wedge x = 0 \Rightarrow 1 = 0$. 但在至少有两个元的有界格中 $1 \neq 0$.

习题 6－3

1. (1) 不是,元数不是 2^n;

(2) 不是,元数不是 2^n;

(3) 不是,有 2^3 个元,但不与$(p(\{a,b,c\}),\leqslant)$ 同构;

(4) 不是,元数不是 2^n.

3. $a = b \Rightarrow (a \wedge b') \vee (a' \wedge b) = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0$;

$$
\begin{aligned}
(a \wedge b') \vee (a' \wedge b) = 0 &\Rightarrow a \wedge b' = 1 = 0' = (a \wedge b')' = a' \vee b, \\
&\Rightarrow 1 = 0' = (a \wedge b')' = a' \vee b \\
&\Rightarrow b = (a')' = a
\end{aligned}
$$

4. (1) $1 + a = (1 \wedge a') \vee (1' \wedge a) = a' \vee 0 = a'$.

(2)
$$
\begin{aligned}
(a \vee b) \wedge (a \wedge b)' &= (a \vee b) \wedge (a' \vee b') \\
&= [(a \vee b) \wedge a'] \vee [(a \vee b) \wedge b'] \\
&= [(a \wedge a') \vee (b \wedge a')] \vee [(a \wedge b') \vee (b \wedge b')]
\end{aligned}
$$

$$= (b \wedge a') \vee (a \wedge b')$$
$$= a + b$$

$$(3)(a \vee b) + ab = [(a \vee b) \wedge (a \wedge b')] \vee [(a \vee b)' \wedge (a \wedge b)]$$
$$= (a + b) \vee [(a' \wedge b') \wedge (a \wedge b)]$$
$$= a + b = a \vee b = a + b - ab$$

习题 7－1

1．7种($G = D_9, \sum_{g \in D_9} |F_g| = 126$).

2．$\frac{1}{24}(n^8 + 17n^4 + 6n^2)$.

习题 7－2

1．(1)1011011(错).

2．

信息码	码词	
	检验数字	信息码
000	000	000
100	110	100
010	011	010
001	111	001
110	101	110
101	001	101
011	100	011
111	010	111

习题 7－3

1．取已知正方体的边长为1．若问题回答是肯定，则$\sqrt[3]{2}$为可构造实数．但$\sqrt[3]{2}$是$\mathbf{Q}[x]$中不可约多项式$x^3 - 2$的根，从而$[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$不是2的幂．

2．取已知圆的半径为1．若问题回答是肯定，则$\sqrt{\pi}$为可构造实数．但π为超越数，从而$\sqrt{\pi}$也是超越数(代数数的平方还是代数数)，故$[\mathbf{Q}(\sqrt{\pi}) : \mathbf{Q}]$不能是2的幂(无限)．

参考文献

1 张禾瑞.近世代数基础.高等教育出版社,1978
2 Jacobson N. Basic Algebra Ⅰ, 2nd Edition. W. H. Freeman & Company, 1985
3 Gilbert W J. Modern Algebra with Applications. John Wiley & Sons, 2004.
4 Hungerford T W. Algebra, Graduate Texts. Springer - Verlag, 1974

[General Information]
书名=近世代数基础
作者=范崇金
页数=108
SS号=12462530
DX号=
出版日期=2008.07
出版社=哈尔滨工程出版社